# Passwordstate Security Administrators Manual

© 2014 Click Studios (SA) Pty Ltd

# Table of Contents


| | | |
|---|---|---|
| | Foreword | 0 |
| Part I | Introduction | 4 |
| Part II | Active Directory Domains | 5 |
| Part III | Auditing | 5 |
| Part IV | Auditing Graphs | 6 |
| Part V | Authorized Web Servers | 7 |
| Part VI | Backups and Upgrades | 7 |
| Part VII | Bad Passwords | 10 |
| Part VIII | Custom Images | 11 |
| Part IX | Email Notification Groups | 11 |
| Part X | Email Templates | 13 |
| Part XI | Emergency Access | 16 |
| Part XII | Export All Passwords | 17 |
| Part XIII | License Information | 17 |
| Part XIV | Menu Access | 17 |
| Part XV | Password Folders | 20 |
| Part XVI | Password Generator Policies | 22 |
| Part XVII | Password Lists | 28 |
| Part XVIII | Password List Templates | 38 |
| Part XIX | Password Strength Policies | 41 |
| Part XX | Reporting | 45 |
| Part XXI | Security Administrators | 46 |


© 2014 Click Studios (SA) Pty Ltd

Part XXII Security Groups 47

Part XXIII System Settings 53

1 Miscellaneous Tab ... 53
2 Password List Options Tab ... 57
3 Password Options Tab ... 61
4 Email Alerts & Options Tab ... 62
5 Proxy & Syslog Servers Tab ... 64
6 Active Directory Options Tab ... 64
7 Authentication Options Tab ... 66
8 Password Synchronization Options ... 79
9 Mobile Access Options ... 80
10 User Acceptance Policy Tab ... 81
11 Check for Updates Tab ... 82
12 Branding Tab ... 82
13 High Availability Options Tab ... 82
14 Allowed IP Ranges Tab ... 83
15 API Key Tab ... 84

Part XXIV User Accounts 84

Part XXV User Account Policies 95

© 2014 Click Studios (SA) Pty Ltd

# 1 Introduction

Welcome to the Passwordstate Security Administrators Manual.

This manual will provide instructions for Security Administrators of Passwordstate to configure user accounts, system wide settings, and various other features which managing the environment.

The following table describes each of the different sections available within the Administration area of Passwordstate.

| | |
|---|---|
| Active Directory Domains | Specify which Active Directory Domains can be queried from within Passwordstate, either for User Accounts or Security Groups |
| Auditing | Provides the ability to query all auditing data within the system, with multiple filtering options, and the ability to export data as well if required |
| Auditing Graphs | Simply a graphical representation of all the auditing data, with similar filtering features |
| Authorized Web Servers | Authorized Web Servers is used to specify which web server host names are authorized to run the Passwordstate web site - used as a mechanism to prevent theft of the database an hosting in a different environment |
| Backups and Upgrades | Allows you to specify settings and a schedule for perform backups of all web files and the database, and also a place to perform In-Place Upgrades of Passwordstate |
| Bad Passwords | A list of password values which are deemed to be 'bad' and can educate your users not to use these values |
| Custom Images | Custom Images are used in two locations in Passwordstate - icons for the Password List themselves, and also for the 'Account Type' field for Password records |
| Email Notification Groups | Can be used to manage email notification settings for a group of individual users accounts, or members of security groups |
| Email Templates | Allows you to customize the emails sent from Passwordstate, or to enable/disable notifications |
| Emergency Access | A separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason |
| Export All Passwords | Allows you to export all Password records from the system to a CSV file |
| License Information | Allows you to enter your license keys for Passwordstate - either Client Access Licenses, Annual Support or High Availability |
| Password Folders | Shows all Password Folders created in Passwordstate |

© 2014 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Password Generator Policies | Create, edit or delete Password Generator Policies. Policies can be associated with one or more Password Lists, and are used as a basis for generating random passwords - of varying complexity |
| Password Lists | Shows all the Shared Password Lists in Passwordstate, and provides various features for administering permissions, moving passwords around, or importing passwords in bulk |
| Password List Templates | Shows all the Password List Templates stored in Passwordstate, which can be used to apply a common set of settings to one or more Password Lists |
| Password Strength Policies | Password Strength Policies are used as a set of rules for determining the strength of a Password. Once a policy is created, it can be applied to one or more Password Lists |
| Reporting | Various reports which can be exported to CSV files |
| Security Groups | Allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/ deny access to various features |
| System Settings | System Settings is used to manage the majority of system wide settings for Passwordstate |
| User Accounts | Allows you to specify the user accounts which are able to access the Passwordstate web site |
| User Account Policies | User Account Policies are used to apply a specify set of settings, to any number of user accounts or security group members |

# 2 Active Directory Domains

The Active Directory Domains screen is where you can specify which domain's user accounts and security groups can authenticate and interact with the Passwordstate website.

If you wish to use multiple domains with Passwordstate, you must have trust relationships configured for the domains, and cross-domain name resolution (DNS) must be working correctly.

Once you have added the relevant domains, you can them import User Accounts or Security Groups as appropriate.

Note: If you are unsure of what NetBIOS Name and LDAP Query String settings to specify, please speak with your Active Directory Administrators for assistance.

# 3 Auditing

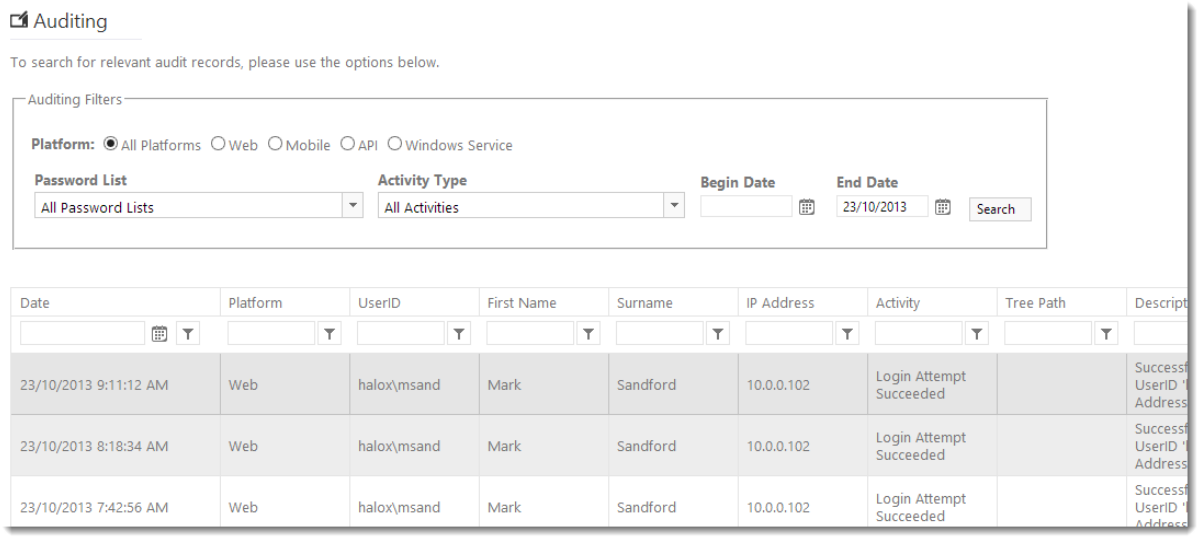
The Auditing screen allows you do report/filter on all auditing data within Passwordstate. Filtering can be done by:

© 2014 Click Studios (SA) Pty Ltd

- Platform - events generated through the web site, the Mobile Client, the API, or functions the Passwordstate Windows Service provides
- Password List - filter on events specific to a selected Password List
- Activity Type - not all audit events relate to passwords i.e. there's audit events for sending emails, failed authentication attempts, etc. To see a complete list of 'Activity Types' ensure the 'Password List' drop-down list has 'All Password Lists' selected
- Beginning and end date - by default, date filtering is not enabled

In addition to reporting on auditing data on the screen, you can export the data for further analysis to a CSV file if required.

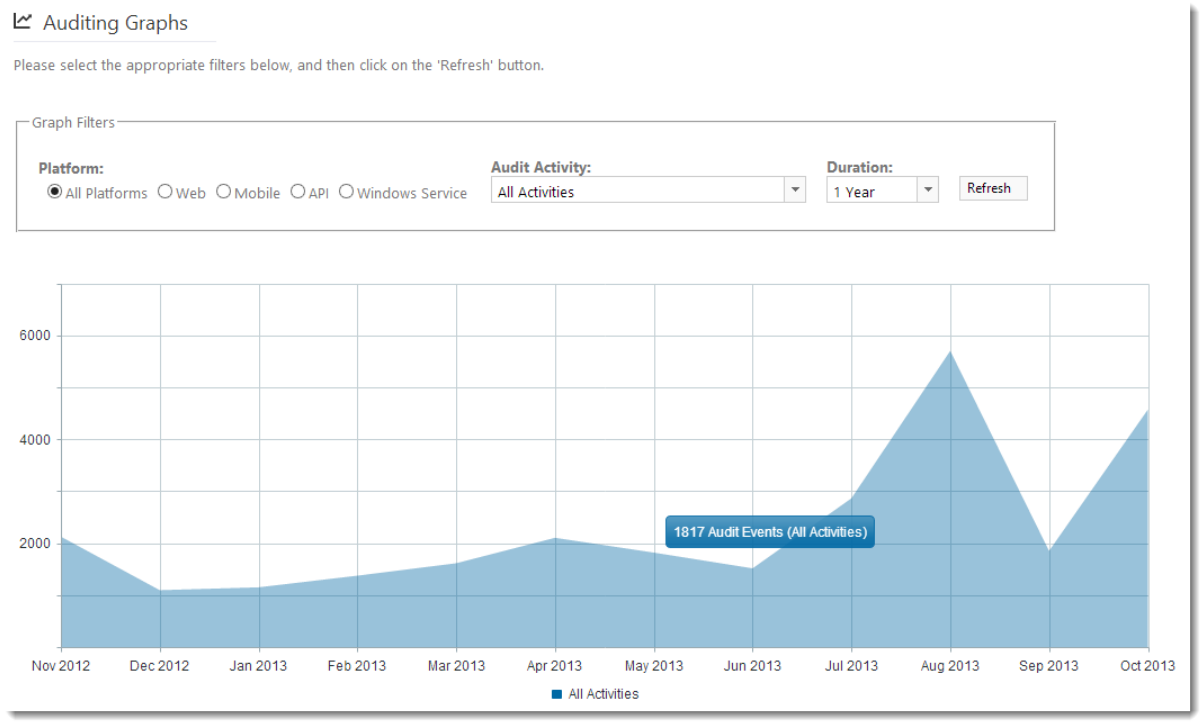
Note 1: You can disable the feature allowing purging of auditing data on the screen System Settings -> Miscellaneous Tab
Note 2: The Telerik Grid and Filter controls here prevent filtering while using special characters - for security reasons. If you're wanting to filter using a backslash (\) here, simply type the backslash twice.




# 4 Auditing Graphs

The Auditing Graphs screen is simply a graphical representation of the auditing data, with similar filtering options. Instead of filtering between dates, you just select a specified period i.e. 1 year, 2 years, etc.

© 2014 Click Studios (SA) Pty Ltd




# 5 Authorized Web Servers

The Authorized Web Servers screen is where you can specify the host names of the web servers which are authorized to host the Passwordstate web site.

The intention of this feature is to prevent the theft of a copy of the database, and hosting it and the web site in an untrusted environment.

Note 1: If you plan on moving your Passwordstate web installation to a new web server, you must first register the host name of the new web server on this screen
Note 2: If you also purchased the High Availability module, you must register the host name of your High Availability instance web server
Note 3: The host names are not case sensitive

# 6 Backups and Upgrades

The Backups and Upgrades screen allows you to specify the settings required to perform backups in Passwordstate, as well execute manual backups and view the status of any backups.

Note 1: You must have backups working correctly, otherwise you will not be able to perform In-Place Upgrades of Passwordstate.
Note 2: The 'Upgrade Now' button takes you to the same screen you would navigate to when clicking on the new build notification hyperlink which 'may' appear at the top of the screen when

© 2014 Click Studios (SA) Pty Ltd

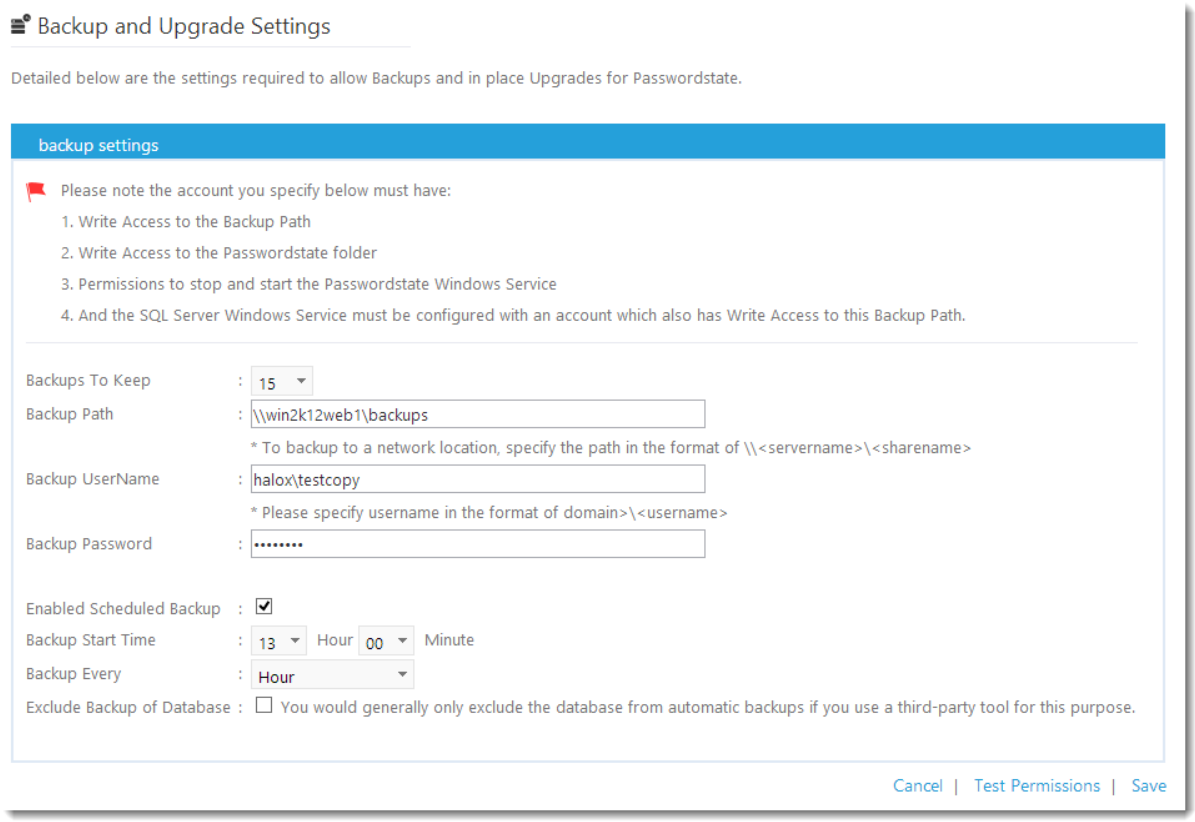
new builds are available

The following instructions will provide some guidance for configuring the backup settings, and other permissions required to backup all the web tier and database files:

## Backup Settings

On the Backup Settings screen, you have the following options available to you:

- How many backups to keep on the file system
- The path to where you would like to store the backups - please use UNC naming conventions here, not a literal path such as c:\backups
- Username and Password required for the backup (below is an explanation of the permissions required)
- Whether you want to enable a regular set-and-forget schedule for the backups to occur
- You can also exclude the database from automatic backups as well, and this is useful if you use a third-party tool to perform SQL Backups which prevents you from executing standard backups
- And finally, what time you would like the scheduled backups to begin, and how often you want a backup to occur


Backup and Upgrade Settings
Detailed below are the settings required to allow Backups and in place Upgrades for Passwordstate.
backup settings
Please note the account you specify below must have:
1. Write Access to the Backup Path
2. Write Access to the Passwordstate folder
3. Permissions to stop and start the Passwordstate Windows Service
4. And the SQL Server Windows Service must be configured with an account which also has Write Access to this Backup Path.
Backups To Keep : 15
Backup Path : \\win2k12web1\backups
* To backup to a network location, specify the path in the format of \\<servername>\<sharename>
Backup UserName : halox\testcopy
* Please specify username in the format of domain>\<username>
Backup Password : ••••••••
Enabled Scheduled Backup :
Backup Start Time : 13 Hour 00 Minute
Backup Every : Hour
Exclude Backup of Database : You would generally only exclude the database from automatic backups if you use a third-party tool for this purpose.
Cancel | Test Permissions | Save

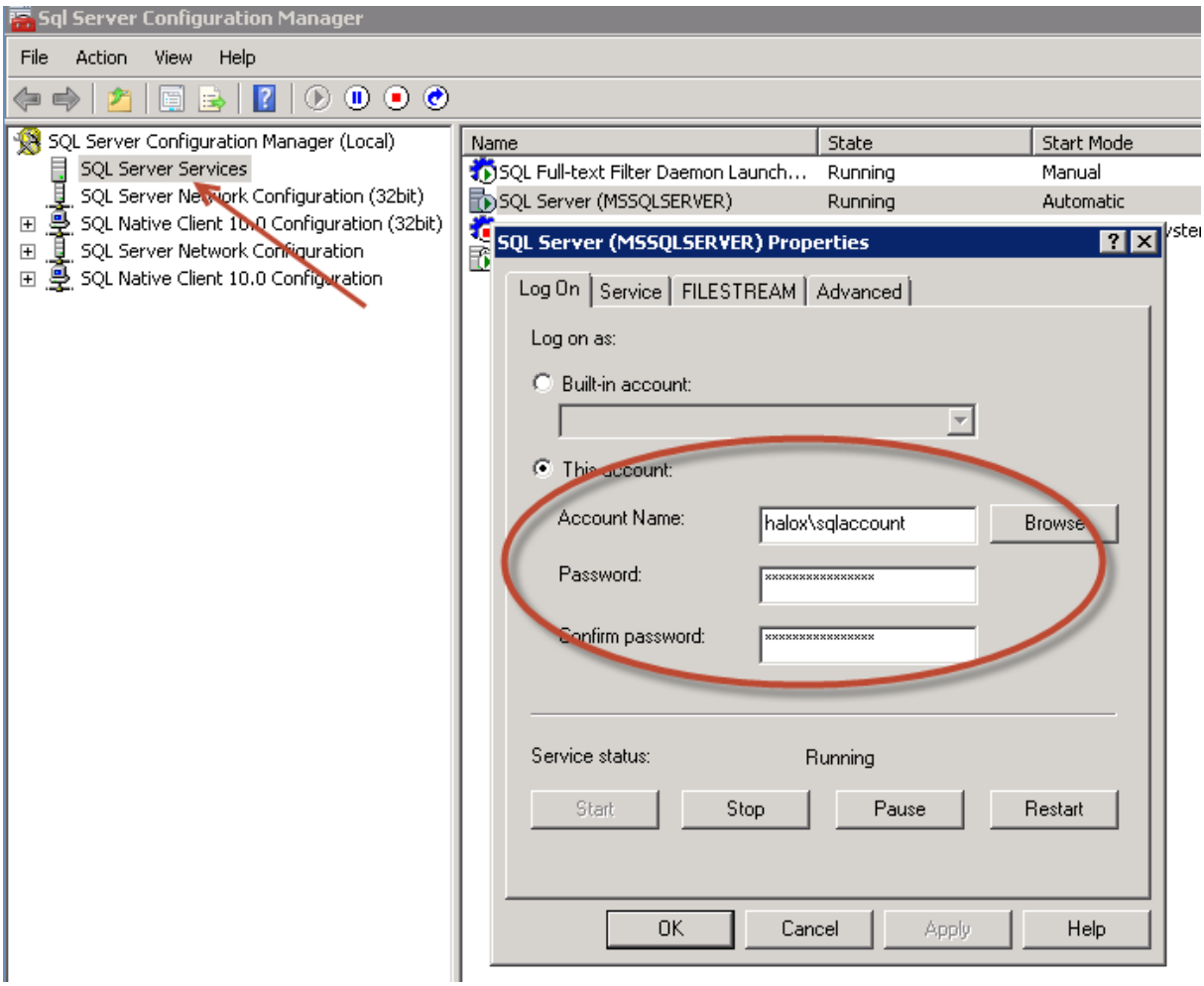
© 2014 Click Studios (SA) Pty Ltd

## Backup Permissions

To allow backups to work through the Passwordstate web interface, you will need to specify an account (domain or Windows account), which has the following permissions:

- Permissions to write to the Backup path you've specified
- Permissions to stop and start the Passwordstate Windows Service on the web server
- Permissions to write to the Passwordstate folder on your web server.

In addition to this, you must configure the SQL Server service to use a domain or Windows account which has permissions to also write to the Backup Path. To do this, you need to open the 'SQL Server Configuration Manager' utility on your database server, click on 'SQL Server Services', and the specify and account as per the next screenshot:




Note: Please ensure you test the upgrade by clicking on the 'Test Permissions' button - this will report any issues with permissions in performing a backup.

© 2014 Click Studios (SA) Pty Ltd

## Automatic Backup Troubleshooting

As every customers' environment can sometimes be slightly different, it's possible you may experience a issues when initially setting up the automatic backups. If this is the case, below is a case scenario of settings which have helped several customers in the past:

- For the backup username we created a domain account called **testcopy**. This account only has Domain User rights, and nothing else
- Backup Share/Folder are located on a Windows Server 2012 server, and the web server is running on a different server altogether
- The Passwordstate Application Pool identity is running as NetworkService (also ensure there are modify NTFS permissions applied to the Passwordstate folder for this account)
- The Share permissions itself is set to full control for 'testcopy' account
- The testcopy account you has modify NTFS permissions to the backup folder
- The testcopy account is set as local administrator on the web server so it can stop/start the Passwordstate Windows Service
- The testcopy account is used for the 'Log On As' identity for the SQL Server service – needed for the SQL Backups (our Security Admin manual shows you how to configure this)
- Testing of permission worked when authenticated to Passwordstate with a domain account which only has Domain User rights on the domain

The following has also helped a few customers as well, who had to assign additional rights on the web server for their equivalent of the testcopy account above – a group policy setting was restricting which domain accounts could use the following setting. The following was required:

- Open a command prompt as Admin
- Type in secpol.msc /s
- Select "Local Policies" in MSC snap in
- Select "User Rights Assignment"
- Right click on "Log on as batch job" and select Properties
- Click "Add User or Group", and include the relevant user account

# 7 Bad Passwords

The Bad Passwords screen allows you to maintain a list of password which are deemed to be bad i.e. common passwords, easy to guess, etc. The intention is to educate your users to ensure they do not use 'Bad' passwords.

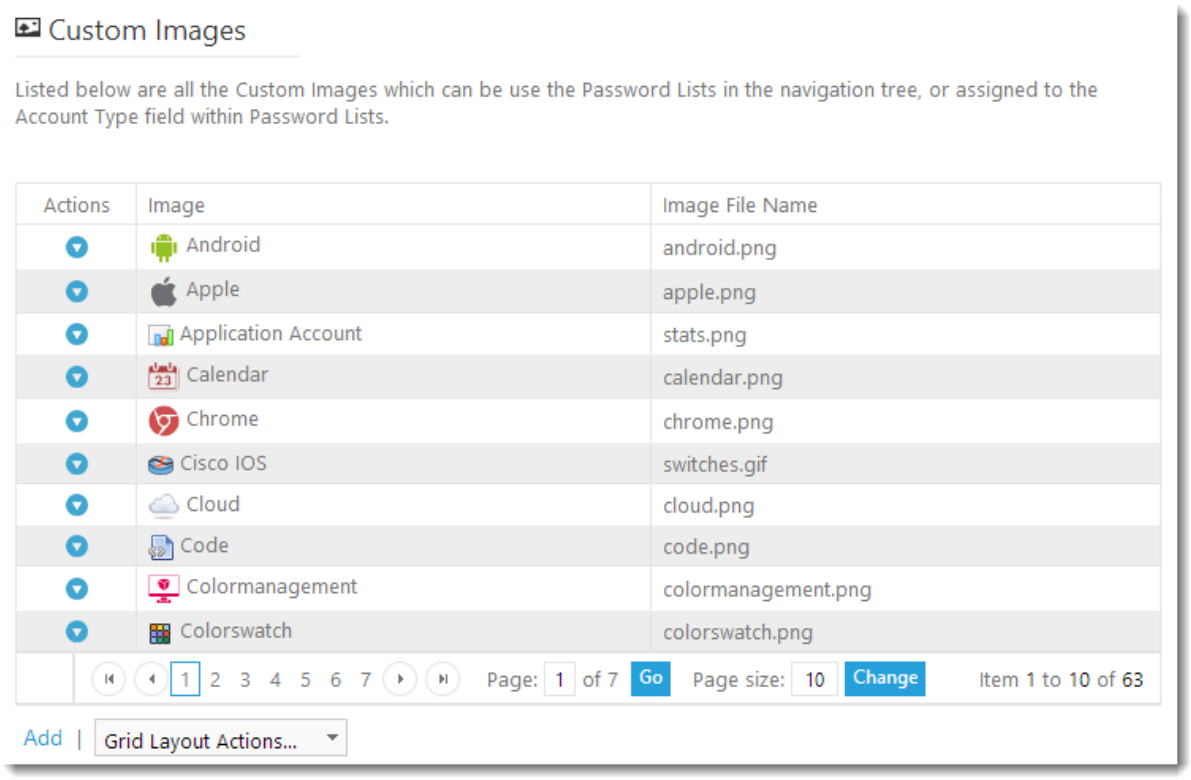
On this screen you can add or delete bad password records, and once you have a list you are happy with, there are options on the screen Administration -> System Settings -> Miscellaneous Tab, and Password Options Tab for notifying your users when bad passwords are detected.

© 2014 Click Studios (SA) Pty Ltd

# 8 Custom Images

The 'Custom Images' screen allows you to upload images which can be used as icons for the Password List themselves, and also for the 'Account Type' field for Password records.

Note 1: All images exist on the web server file system in the path <Passwordstate Folder>\images\LookupImages, and are also stored within the Passwordstate database as well. Deleting them from the file system will caused them to be recreated once the Passwordstate Windows Service is next restarted.
Note 2: It is recommended you keep these images relatively small, inline with the size of the supplied images, otherwise it can distort the view of Password Lists in the Navigation Tree, and anywhere Account Type images are displayed



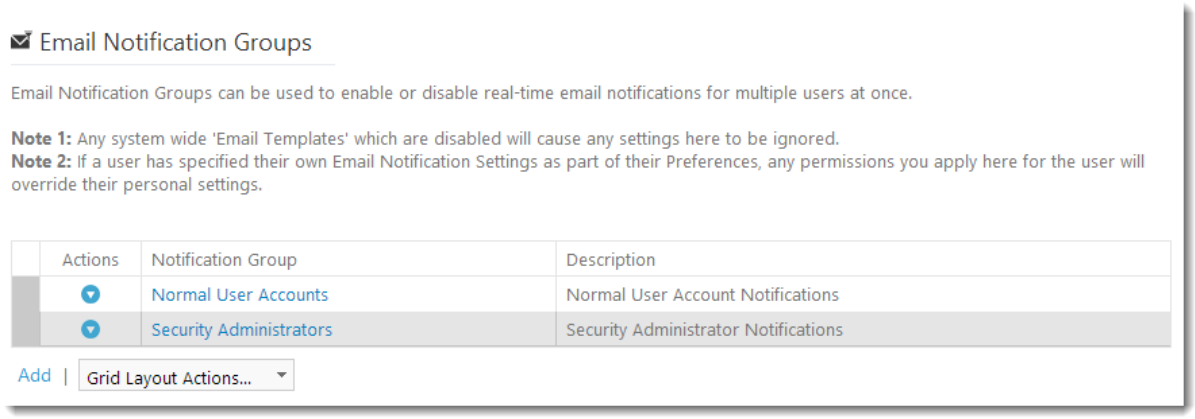

# 9 Email Notification Groups

The Email Notification Groups screen is used to manage email notification settings for a group of individual users accounts, or members of security groups.

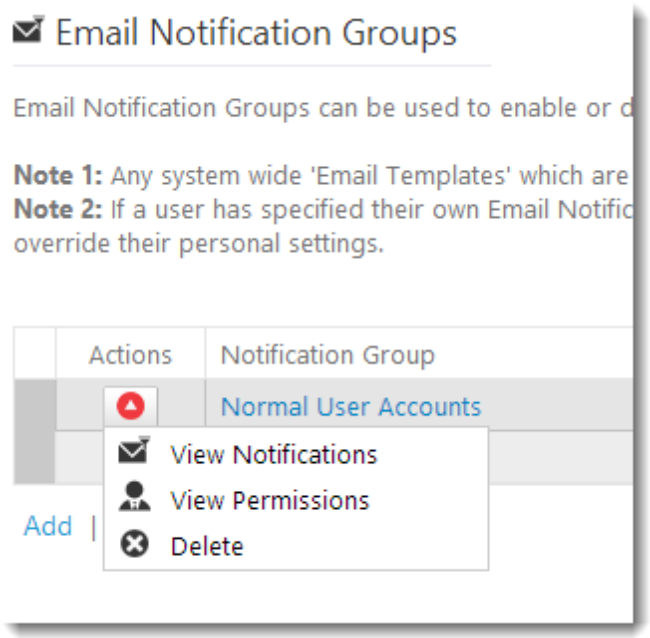
Using Email Notification Groups, you can specify which email notifications certain users receive, or don't receive i.e. you may wish to have certain notifications enabled for Security Administrators, but disabled for 'normal' user accounts in Passwordstate.

© 2014 Click Studios (SA) Pty Ltd

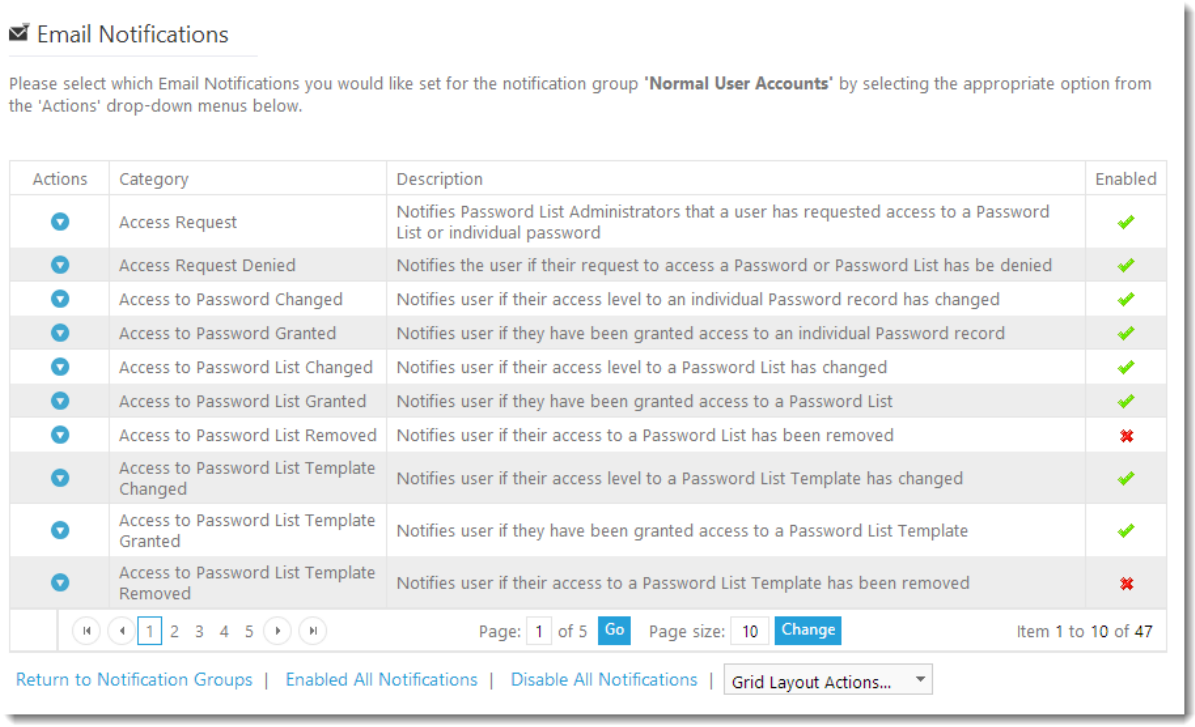
Note 1: Any system wide Email Templates which are disabled will cause any settings here to be ignored
Note 2: If a user has specified their own Email Notification Settings as part of their Preferences, any permissions you apply here for the user will override their personal settings
Note 3: If you have more than one Notification Group created for a user, any disabled email categories will over-ride any enabled ones (be careful applying duplicates for a user)


Email Notification Groups
Email Notification Groups can be used to enable or disable real-time email notifications for multiple users at once.
Note 1: Any system wide 'Email Templates' which are disabled will cause any settings here to be ignored.
Note 2: If a user has specified their own Email Notification Settings as part of their Preferences, any permissions you apply here for the user will override their personal settings.
Actions
Notification Group
Description
Normal User Accounts
Normal User Account Notifications
Security Administrators
Security Administrator Notifications
Add
Grid Layout Actions...

Once you have created a Notification Group, you can then assign permissions for who is affected by the settings, and which emails are either enabled or disabled. You do this by clicking on the appropriate menu item in the 'Actions' drop-down menu.


Email Notification Groups
Email Notification Groups can be used to enable or d
Note 1: Any system wide 'Email Templates' which are
Note 2: If a user has specified their own Email Notific
override their personal settings.
Actions
Notification Group
Normal User Accounts
View Notifications
View Permissions
Delete
Add

© 2014 Click Studios (SA) Pty Ltd


Email Notifications
Please select which Email Notifications you would like set for the notification group 'Normal User Accounts' by selecting the appropriate option from the 'Actions' drop-down menus below.
Actions
Category
Description
Enabled
Access Request
Notifies Password List Administrators that a user has requested access to a Password List or individual password
Access Request Denied
Notifies the user if their request to access a Password or Password List has be denied
Access to Password Changed
Notifies user if their access level to an individual Password record has changed
Access to Password Granted
Notifies user if they have been granted access to an individual Password record
Access to Password List Changed
Notifies user if their access level to a Password List has changed
Access to Password List Granted
Notifies user if they have been granted access to a Password List
Access to Password List Removed
Notifies user if their access to a Password List has been removed
Access to Password List Template Changed
Notifies user if their access level to a Password List Template has changed
Access to Password List Template Granted
Notifies user if they have been granted access to a Password List Template
Access to Password List Template Removed
Notifies user if their access to a Password List Template has been removed
1 2 3 4 5
Page: 1 of 5 Go
Page size: 10 Change
Item 1 to 10 of 47
Return to Notification Groups | Enabled All Notifications | Disable All Notifications | Grid Layout Actions...

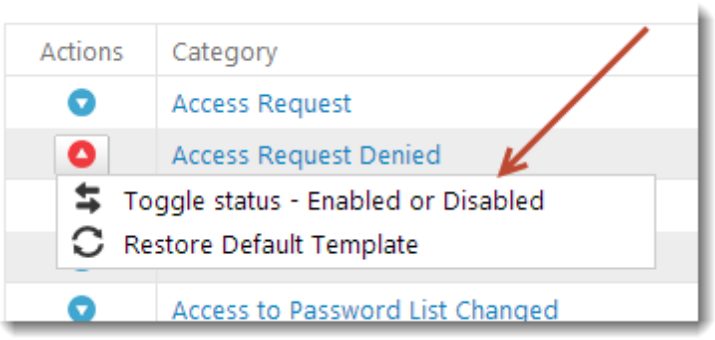
# 10 Email Templates

The Email Templates screen allows you to customize the emails sent from Passwordstate, or to enable/disable notifications as required.

## Enabling/Disabling Email Notifications

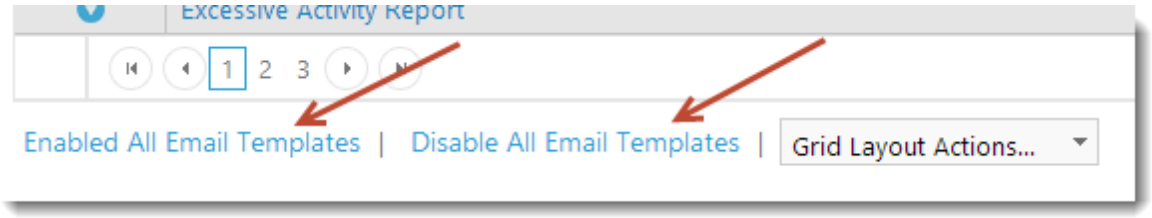
You can enable/disable email notifications in one of either two ways:

1. Individually by the appropriate 'Actions' drop-down menu




2. Enabling/disabling all email notifications at once by clicking on the the appropriate 'Enable All' or 'Disable All' buttons at the bottom of the grid

© 2014 Click Studios (SA) Pty Ltd



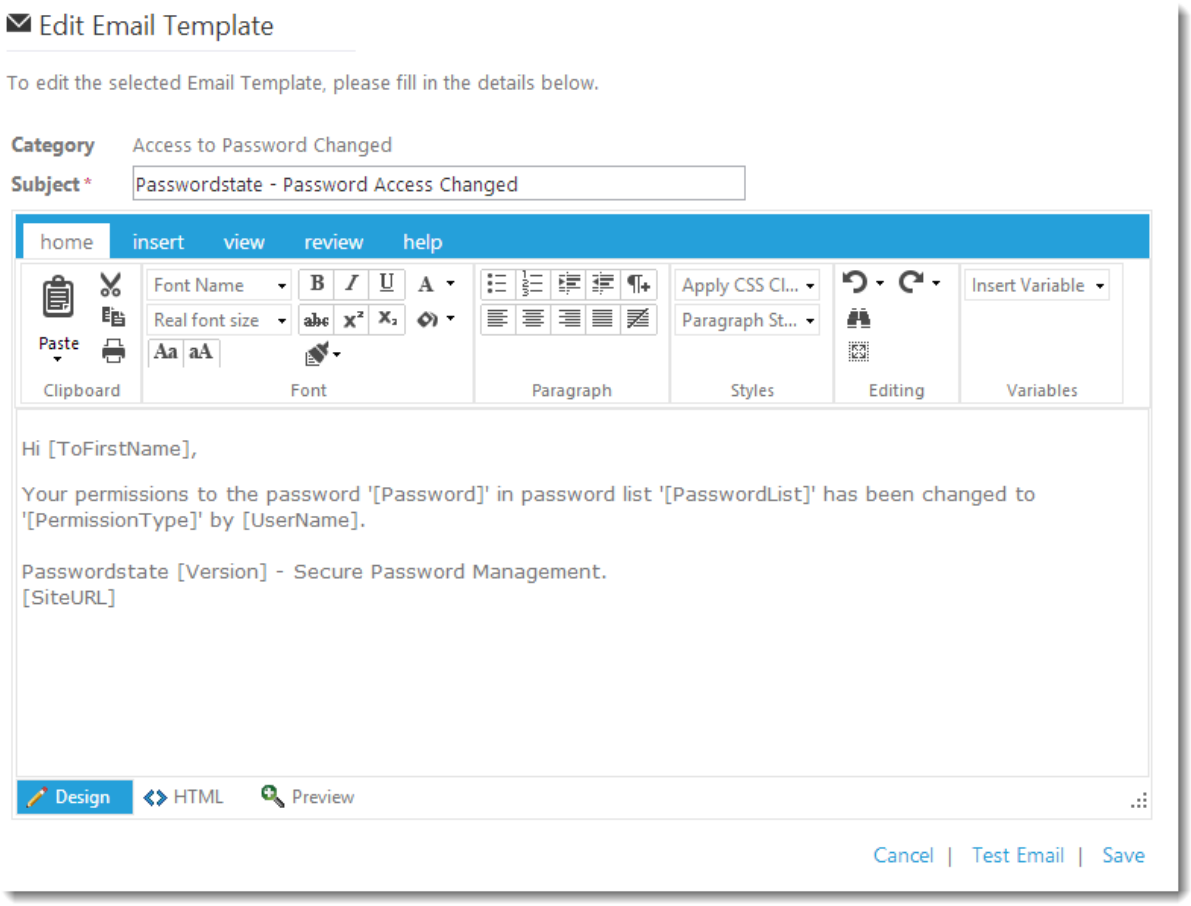

## Editing Email Template Content

By clicking on the 'Category' hyperlink in the grid, you can edit the content of the email template - specifying your own words, and formatting options.

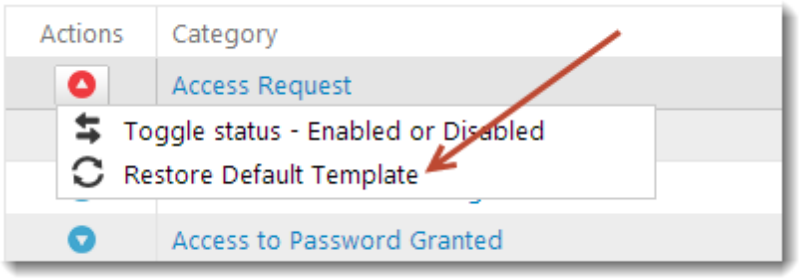
At the top right-hand side of the Editor you will notice the 'Variables' tab/ribbon bar. From this drop-down list, you can insert the following variables into your email templates:

- ToFirstName - the First Name of the user who is receiving the email
- ToUserID - the UserID of the user who is receiving the email
- SiteURL - the URL of your Passwordstate web site
- PermissionType - the permission being applied to a Password List or Password record for the user
- PasswordList - the name of the Password List
- Password - the title of the Password record
- Version - the Version number of your Passwordstate install
- UserName - A combination of the Firstname and Username of the user
- ExpiresAt - the date at which a users permissions to a Password List or Password will be removed
- AdditionalBodyText - reserved by Click Studios for various custom text messages
- AuthenticationMethod - which Authentication method was used for authenticated to the Passwordstate web site, or to a Password List

© 2014 Click Studios (SA) Pty Ltd




If while editing the contents or formatting of an Email Template you decide you don't like the changes you've made, you can restore back to the original content as supplied by Click Studios by selecting 'Restore Default Template' from the appropriate Actions drop-down menu.




## Testing and Troubleshooting Emails being Sent

When editing a Password List template, there is a button called 'Test Email'. This button will test sending the email template to your own email account. This testing is different however to how emails are normally sent from Passwordstate - normally records are added to the database, and the Passwordstate Windows Service checks and send emails every minute. This 'Test Email' button sends directly from the web site, and does not use the Passwordstate Windows Service.

© 2014 Click Studios (SA) Pty Ltd

If emails are queuing up and not being sent as expected, the following suggestions may help to troubleshoot why:

1. Check you have correctly specified your email server's settings on the screen Administration -> System Settings -> Email Alerts & Options Tab
2. Ensure the Passwordstate Windows Service is started
3. Check the event log on your web server to see if any errors are being reported as to why emails aren't being sent - look for the Source of 'Passwordstate Service'
4. Check there aren't any Email Templates disabled, either on the screen Email Templates, or Email Notification Groups, or possibly the user has disabled an email notification in their Preferences area

# 11 Emergency Access

The Emergency Access screen allows you to specify a password for a separate 'Security Administrator' role login which can be used in the event other accounts are locked out, or inaccessible for any reason.

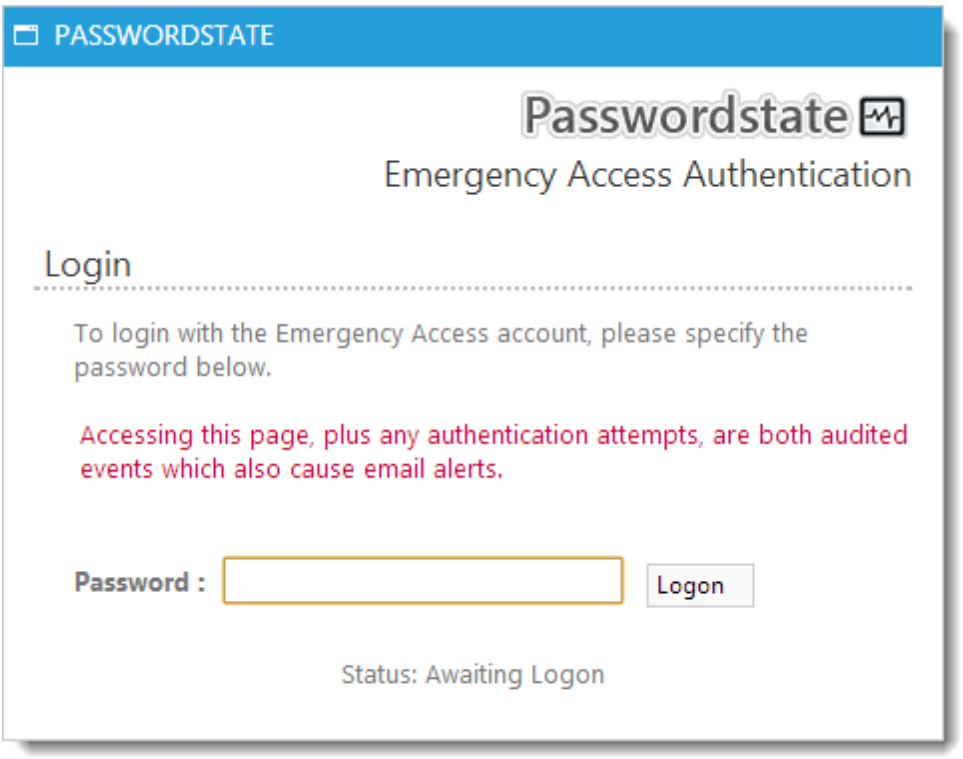
A couple of scenarios where this would be applicable is:

- You have issues with authenticating on your domain, and can no longer authenticate to Passwordstate using your normal domain account
- Someone has accidentally deleted or disabled all Security Administrator accounts, and no-one is able to administer all the settings for Passwordstate

The Emergency Access URL is HTTPS://<Your Passwordstate URL>/Emergency

Note 1: Simply browsing to the Emergency Access URL will generate audit records, and notify Security Administrators via email
Note 2: Navigating to the page Administration -> Emergency Access will also generate audit records, and notify Security Administrators via email
Note 3: Once you've logged in with this account, you will have access to the Administration area of Passwordstate

© 2014 Click Studios (SA) Pty Ltd


PASSWORDSTATE
Passwordstate
Emergency Access Authentication
Login
To login with the Emergency Access account, please specify the password below.
Accessing this page, plus any authentication attempts, are both audited events which also cause email alerts.
Password :
Logon
Status: Awaiting Logon

# 12 Export All Passwords

The Export All Passwords screen allows you to export all Password records from the system to a CSV file.

Note 1: If you choose to export all passwords to a csv file, they must be stored away somewhere securely as the passwords appear as plain-text in the csv file
Note 2: In addition to the normal audit record added to indicate all Passwords have been exports, one 'Password Viewed' audit record will be added per password record - required for compliance reasons for some organizations

# 13 License Information

The License Information screen simply allows you to update your license registration keys for Passwordstate.

Note: When you purchase your renewal for Annual Support + Upgrades, it's import you update your 'Annual Support' registration key on this screen, otherwise you will be prevented from upgrading to new builds of Passwordstate.

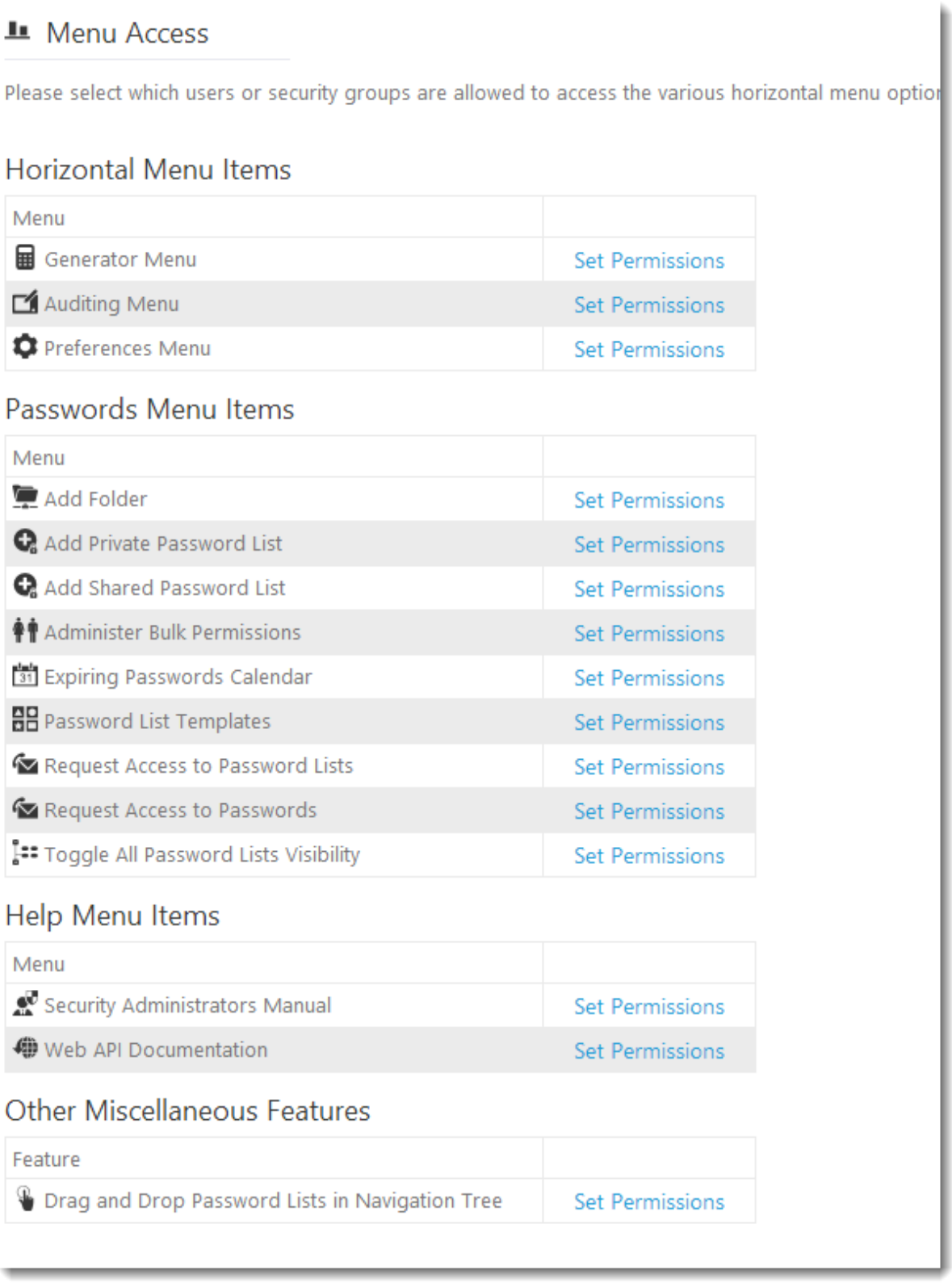
# 14 Menu Access

The Menu Access screen allows you to specify which users or security groups are allowed to access the various horizontal menu options at the bottom of the Passwordstate screen.

© 2014 Click Studios (SA) Pty Ltd

By clicking on the appropriate 'Set Permissions' button, you can allow all users to have access, or just the ones you specify. If a user doesn't have access, then menu option will be disabled for them.

© 2014 Click Studios (SA) Pty Ltd



## Menu Access

Please select which users or security groups are allowed to access the various horizontal menu optio

### Horizontal Menu Items

| Menu | |
|---|---|
| Generator Menu | Set Permissions |
| Auditing Menu | Set Permissions |
| Preferences Menu | Set Permissions |

### Passwords Menu Items

| Menu | |
|---|---|
| Add Folder | Set Permissions |
| Add Private Password List | Set Permissions |
| Add Shared Password List | Set Permissions |
| Administer Bulk Permissions | Set Permissions |
| Expiring Passwords Calendar | Set Permissions |
| Password List Templates | Set Permissions |
| Request Access to Password Lists | Set Permissions |
| Request Access to Passwords | Set Permissions |
| Toggle All Password Lists Visibility | Set Permissions |

### Help Menu Items

| Menu | |
|---|---|
| Security Administrators Manual | Set Permissions |
| Web API Documentation | Set Permissions |

### Other Miscellaneous Features

| Feature | |
|---|---|
| Drag and Drop Password Lists in Navigation Tree | Set Permissions |

© 2014 Click Studios (SA) Pty Ltd

# 15 Password Folders

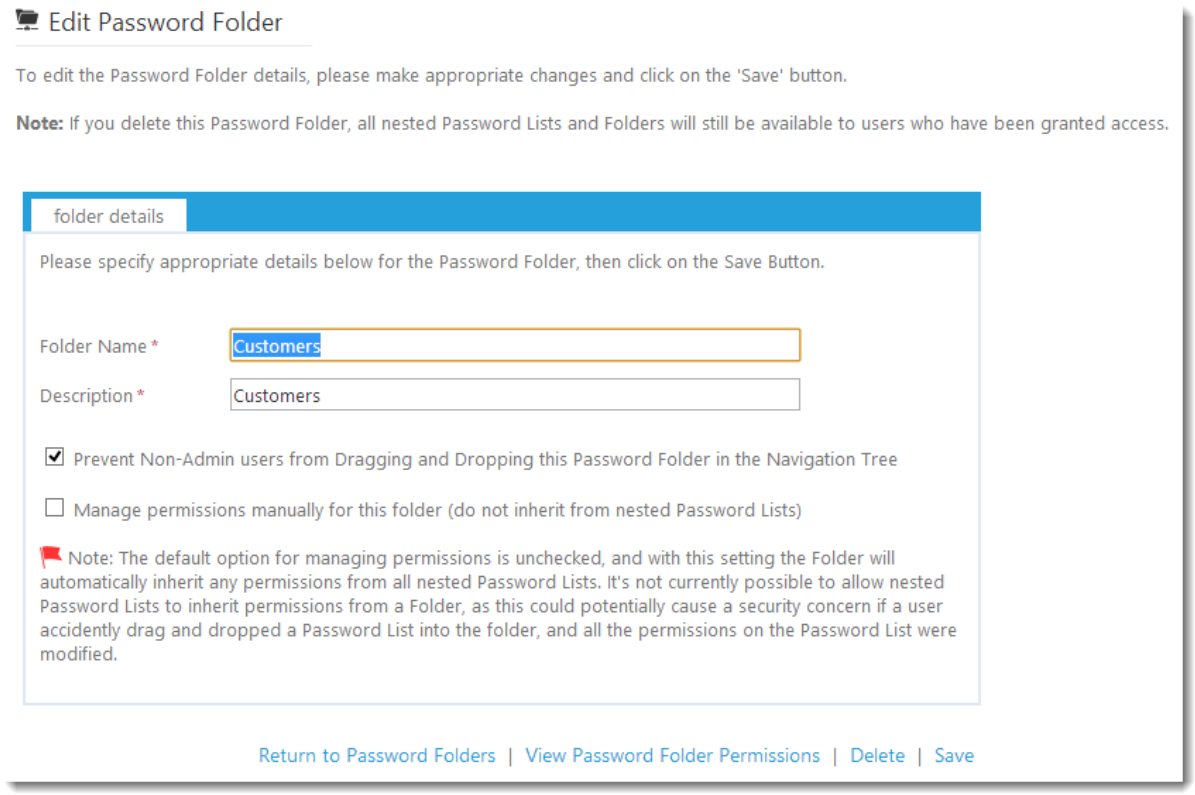
The Password Folders screen show you all the Password Folders which have been created in Passwordstate. From this screen you can:

## Edit Password Folder Details, View Permissions & Delete the Folder

By clicking on the 'Password Folder' hyperlink you see in the grid, you will be taken to a screen where you can perform the following actions on the Folder:

- Edit name, description and settings
- View Permissions - by default, permissions are automatically applied to Folders. The permissions applied to Password Lists are propagated up through the Navigation Tree, and applied to any Folders above it. The only exception to this is when the 'Manager Permissions Manually' option is selected for a Folder
- Delete the folder - deleting a folder will not delete any nested Folders or Password Lists

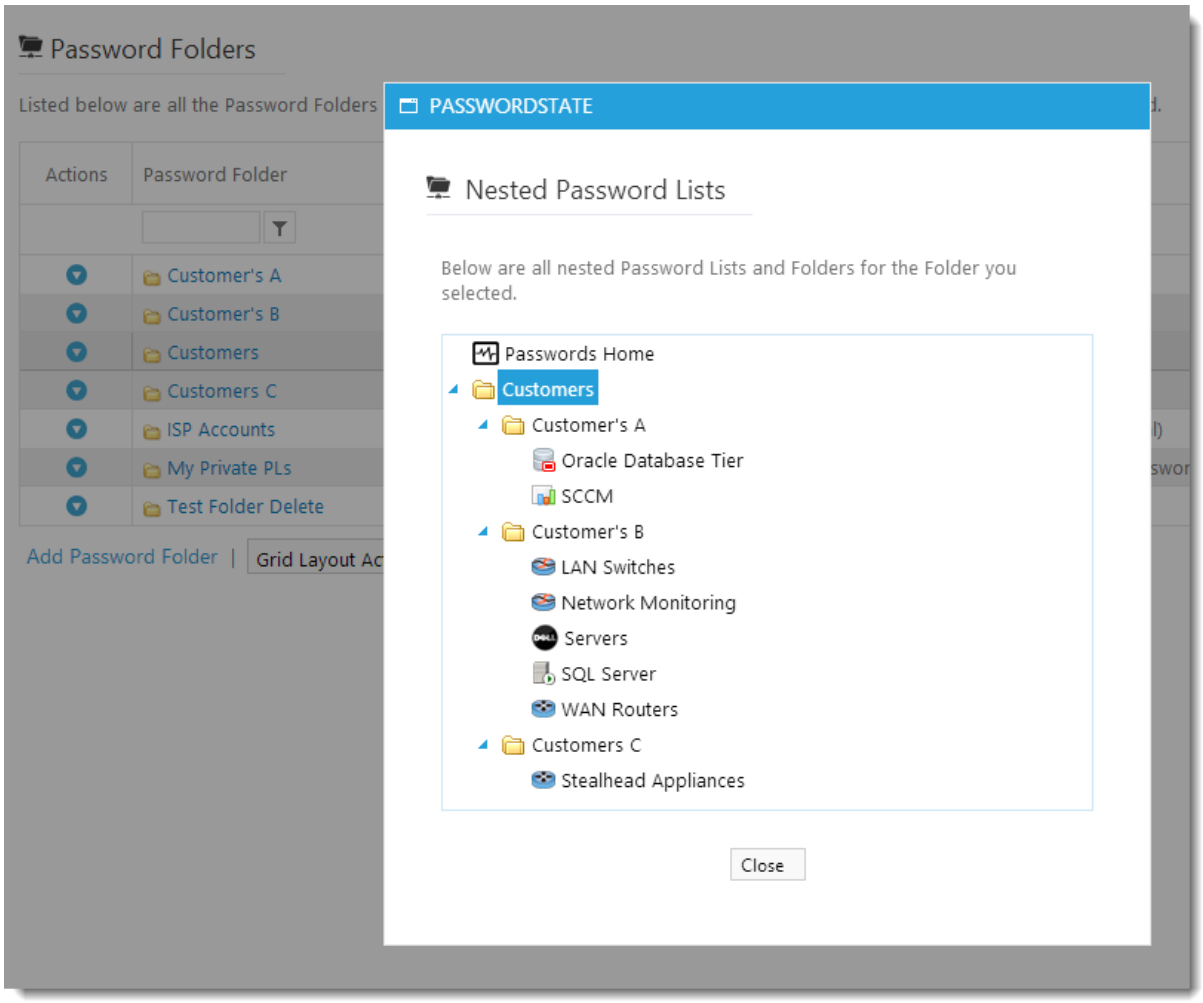
Note: The default option for managing permissions is unchecked, and with this setting the Folder will automatically inherit any permissions from all nested Password Lists. It's not currently possible to allow nested Password Lists to inherit permissions from a Folder, as this could potentially cause a security concern if a user accidently drag and dropped a Password List into the folder, and all the permissions on the Password List were modified.


Edit Password Folder
To edit the Password Folder details, please make appropriate changes and click on the 'Save' button.
Note: If you delete this Password Folder, all nested Password Lists and Folders will still be available to users who have been granted access.
folder details
Please specify appropriate details below for the Password Folder, then click on the Save Button.
Folder Name *
Customers
Description *
Customers
Prevent Non-Admin users from Dragging and Dropping this Password Folder in the Navigation Tree
Manage permissions manually for this folder (do not inherit from nested Password Lists)
Note: The default option for managing permissions is unchecked, and with this setting the Folder will automatically inherit any permissions from all nested Password Lists. It's not currently possible to allow nested Password Lists to inherit permissions from a Folder, as this could potentially cause a security concern if a user accidently drag and dropped a Password List into the folder, and all the permissions on the Password List were modified.
Return to Password Folders | View Password Folder Permissions | Delete | Save

© 2014 Click Studios (SA) Pty Ltd

## View Nested Password Lists

By selecting the option 'View Nested Password Lists' from the appropriate Actions drop-down menu, a popup screen will appear showing all Folders and Password Lists nested beneath the one you've chosen.

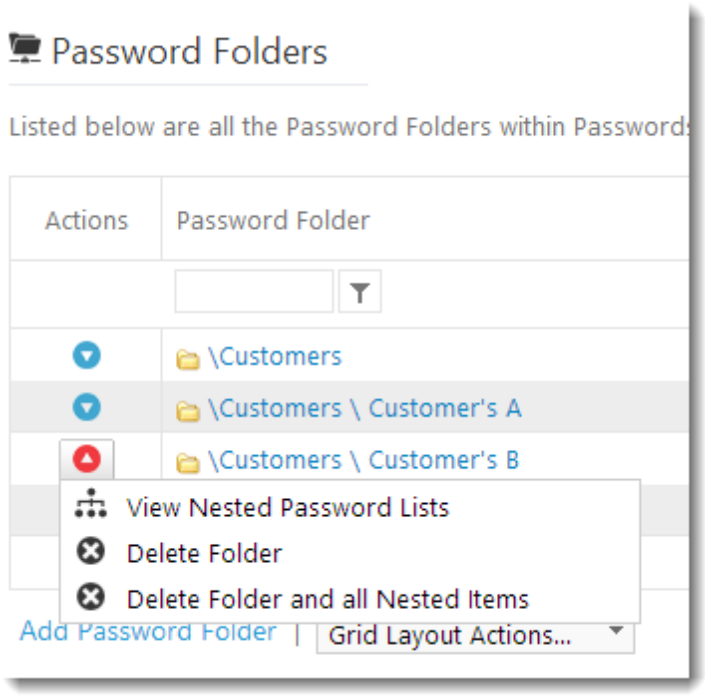



## Deleting Folders

Also in the 'Actions' menu are two options for deleting a folder:

- Delete Folder - will delete just the folder, and nothing else. The Navigation Menu will look different to your users once you've done this, as it will need to rearrange any nested Password Lists/Folders
- Delete Folder and all Nested Items - Please use with caution, as this will deleted all nested Password Lists/Folders, including all associated passwords

© 2014 Click Studios (SA) Pty Ltd




# 16 Password Generator Policies

The Password Generator Policies screen allows you to create and manage multiple settings for the Password Generator, which can then be applied to one or more Password Lists.

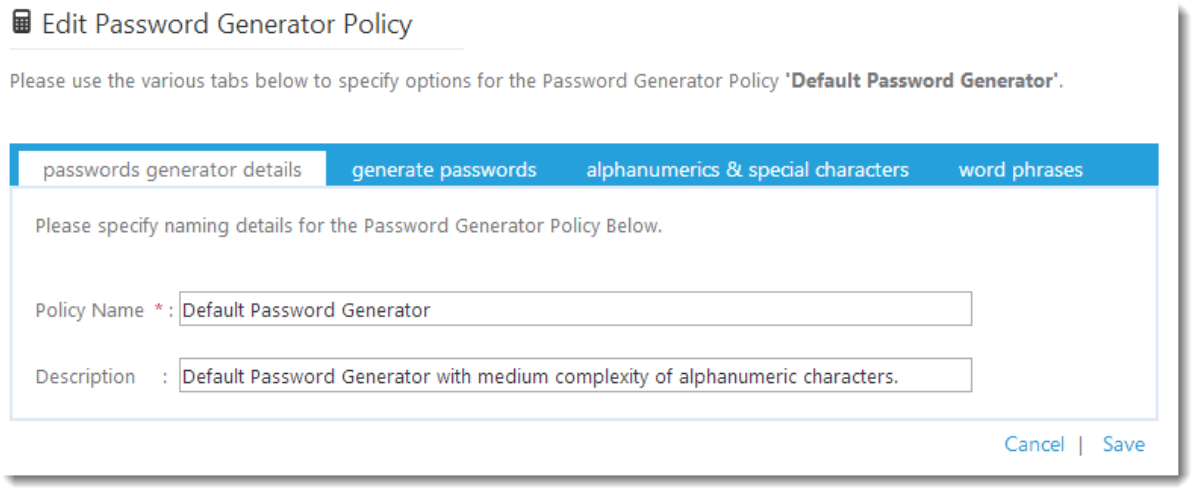
Note: The Default Password Generator policy cannot be deleted - it can be renamed and its settings modified, but it cannot be deleted.

When adding or editing a Password Generator Policy, you have the following options available to you:

## Password Generator Details

Edit the name and description for the Policy.

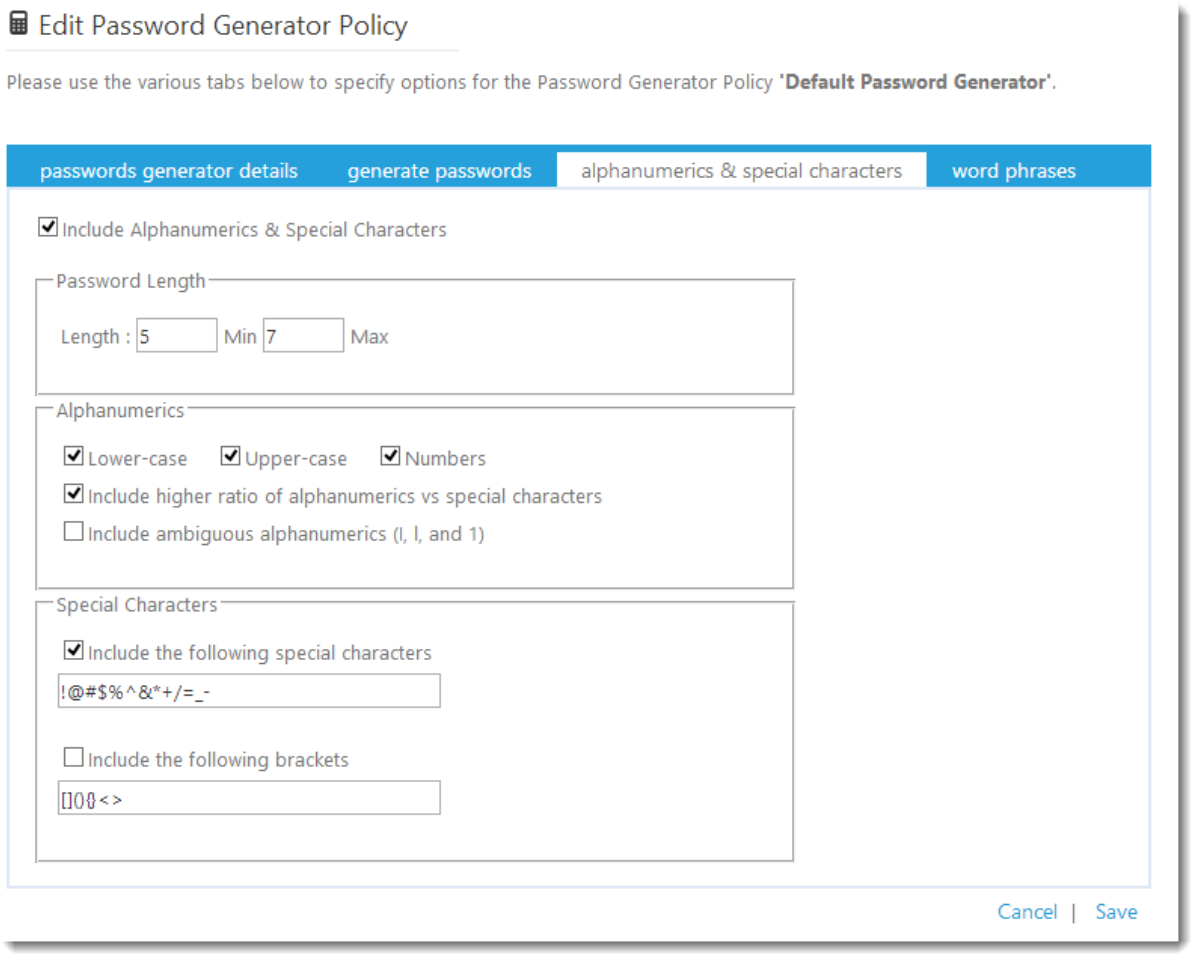
© 2014 Click Studios (SA) Pty Ltd


Edit Password Generator Policy
Please use the various tabs below to specify options for the Password Generator Policy 'Default Password Generator'.
passwords generator details
generate passwords
alphanumerics & special characters
word phrases
Please specify naming details for the Password Generator Policy Below.
Policy Name * : Default Password Generator
Description : Default Password Generator with medium complexity of alphanumeric characters.
Cancel | Save

## Alphanumerics & Special Characters

The Alphanumeric & Special Characters tab allows you to specify the desired length of the password you wish to generate, as well as settings for letters, numbers, special characters and various forms of brackets.

© 2014 Click Studios (SA) Pty Ltd

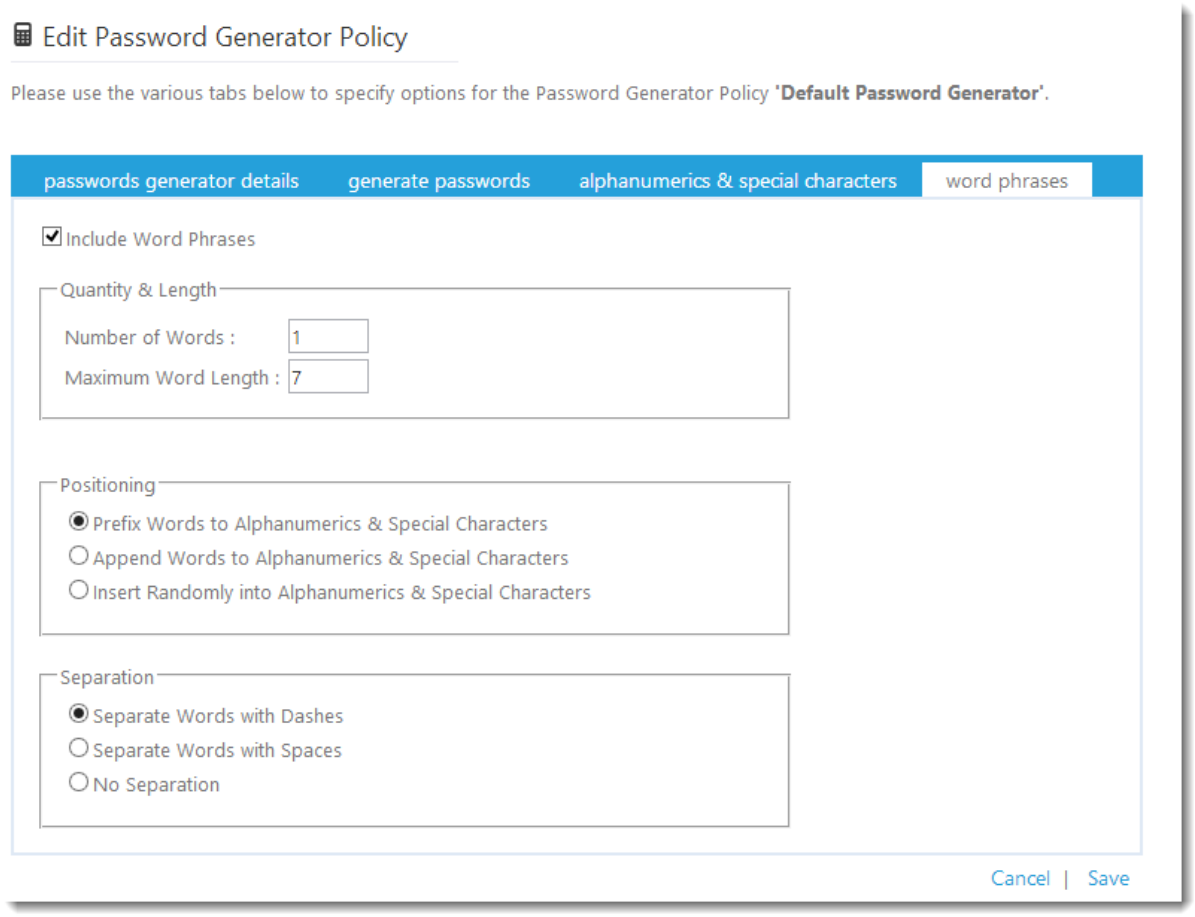



## Word Phrases

The Word Phrases tab allows you to insert a random word at the beginning of the password, somewhere in the middle, or at the end. You can specify how many words to create, what length, and what form of separation you would like between the word and the rest of the random password - either dashes, spaces or nothing.

Passwordstate has 10,000 different words it can choose from, all of different lengths.

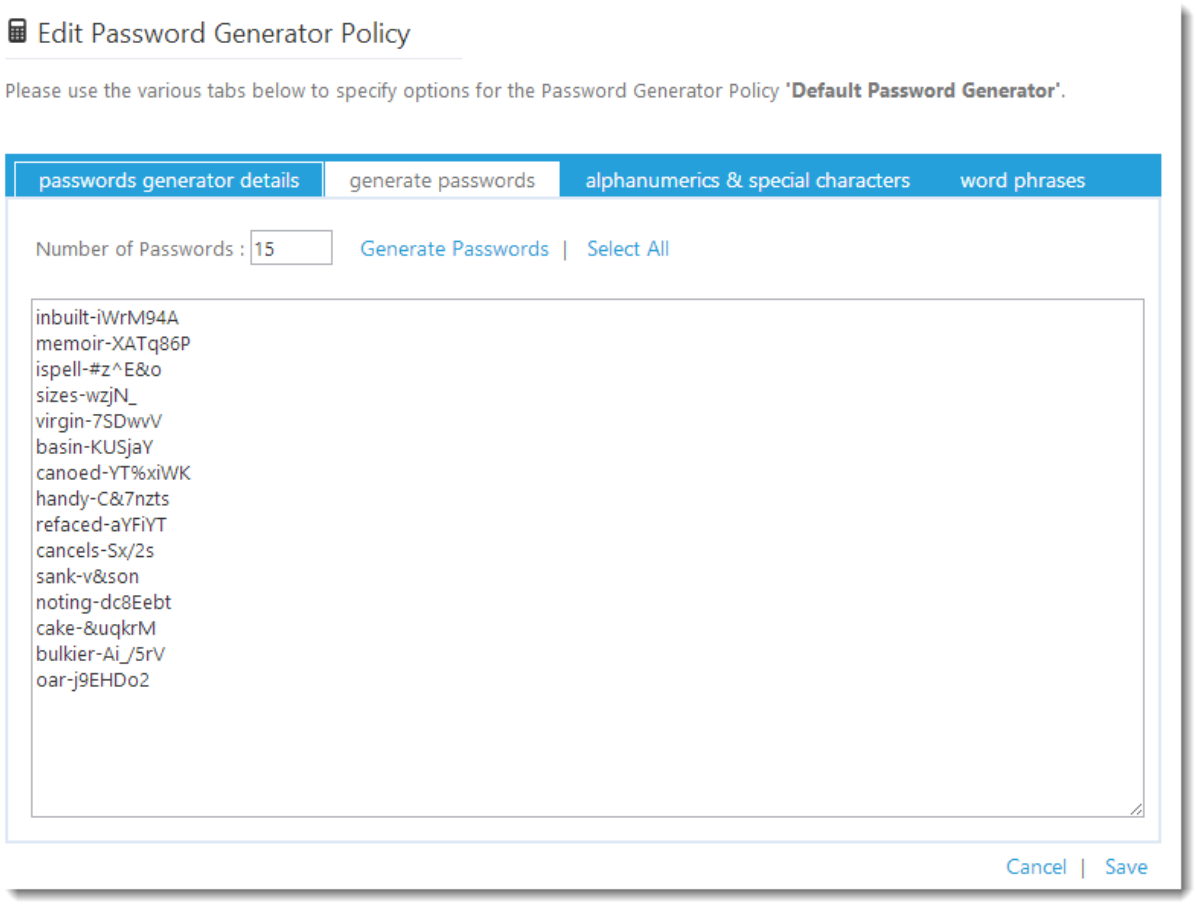
© 2014 Click Studios (SA) Pty Ltd


Edit Password Generator Policy
Please use the various tabs below to specify options for the Password Generator Policy 'Default Password Generator'.
passwords generator details
generate passwords
alphanumerics & special characters
word phrases
Include Word Phrases
Quantity & Length
Number of Words : 1
Maximum Word Length : 7
Positioning
Prefix Words to Alphanumerics & Special Characters
Append Words to Alphanumerics & Special Characters
Insert Randomly into Alphanumerics & Special Characters
Separation
Separate Words with Dashes
Separate Words with Spaces
No Separation
Cancel | Save

## Generate Passwords

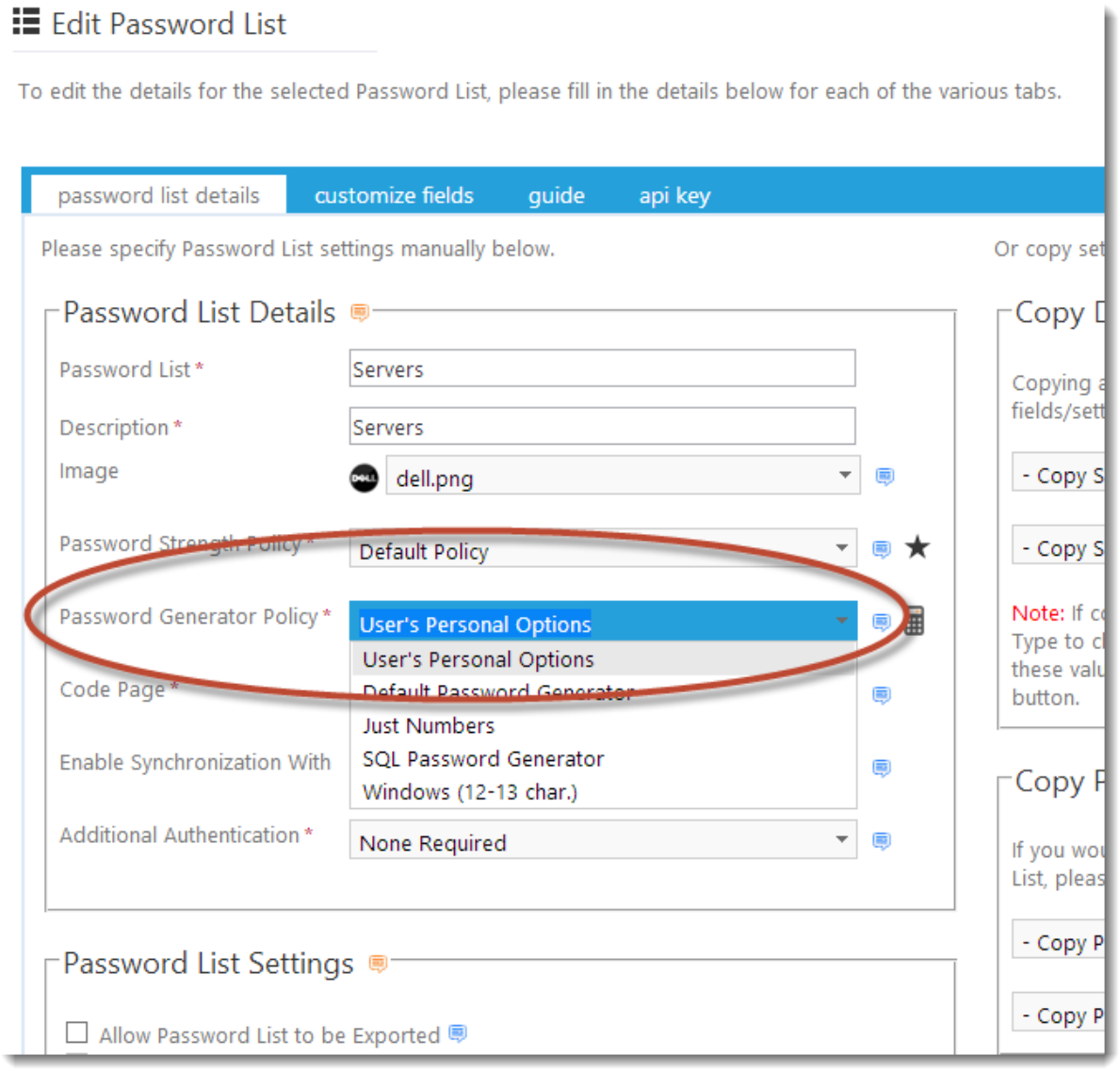
The Generate Passwords tab allows you to test the settings you have specified on the other tabs, and also generate any number of random passwords based on your settings.

© 2014 Click Studios (SA) Pty Ltd




Once a Password Generator Policy has been created, it can be assigned to a Password List or Password List Template, by editing the appropriate settings, as per this screenshot below. When your users now click on the icon, the random password generated will be based on the selected Password Generator Policy.

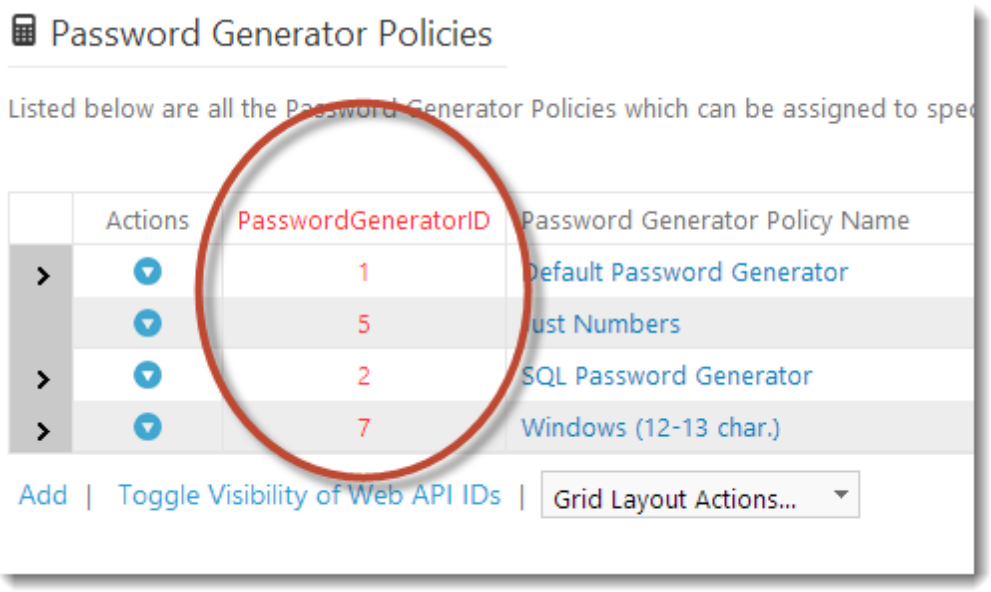
© 2014 Click Studios (SA) Pty Ltd




## Toggle Visibility of Web API IDs

When using the Passwordstate Web API, there are certain API calls which can also automatically generate passwords. In order to specify which policy to use when making these API calls, you need to know the PasswordGeneratorID value - a unique identifier for each policy. By clicking on the 'View Visibility of Web API IDs' button, you will see the PasswordGeneratorID values as per this screenshot:

© 2014 Click Studios (SA) Pty Ltd




# 17 Password Lists

The Password Lists screen shows **all Shared Password Lists** created in Passwordstate, regardless of whether your account has Administrative rights to the Password Lists or not.

From this screen, the following features are available:

## Navigating to, and viewing a Password List

By clicking on one of the 'Password List' hyperlinks in the grid, you will be redirected to the appropriate Password List screen.

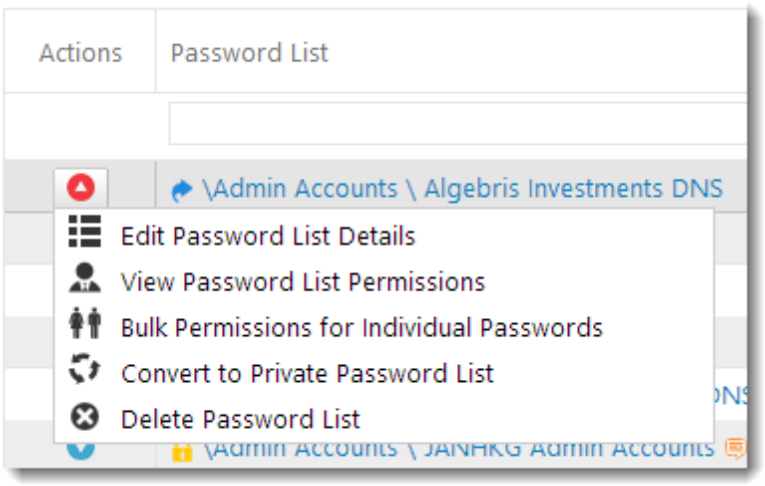
Note: When you view the Password Lists screen via Administration -> Password Lists, the passwords themselves will be hidden, and most features will be disabled. The intention of navigating this way is to fix any permissions issues on the Password List, or correcting any possible settings issues. The following warning will be displayed on the screen when navigating to a Password List this way:

Note: As you have navigated to this page from the 'Administration' area, certain functions to view or modify passwords have been disabled.

## Actions Menu Items

By clicking on one of the 'Action' menus for a Password List, there will be various features available to you, which are explained below.

© 2014 Click Studios (SA) Pty Ltd




## Actions Menu - Edit Password List Details

By clicking on the 'Edit Password List Details' menu option in the 'Actions' drop-down menu, you will be able to edit settings for the selected Password List.

Note: Please refer to the Passwordstate User Manual for detailed instructions on settings which can be applied to a Password List or Template.

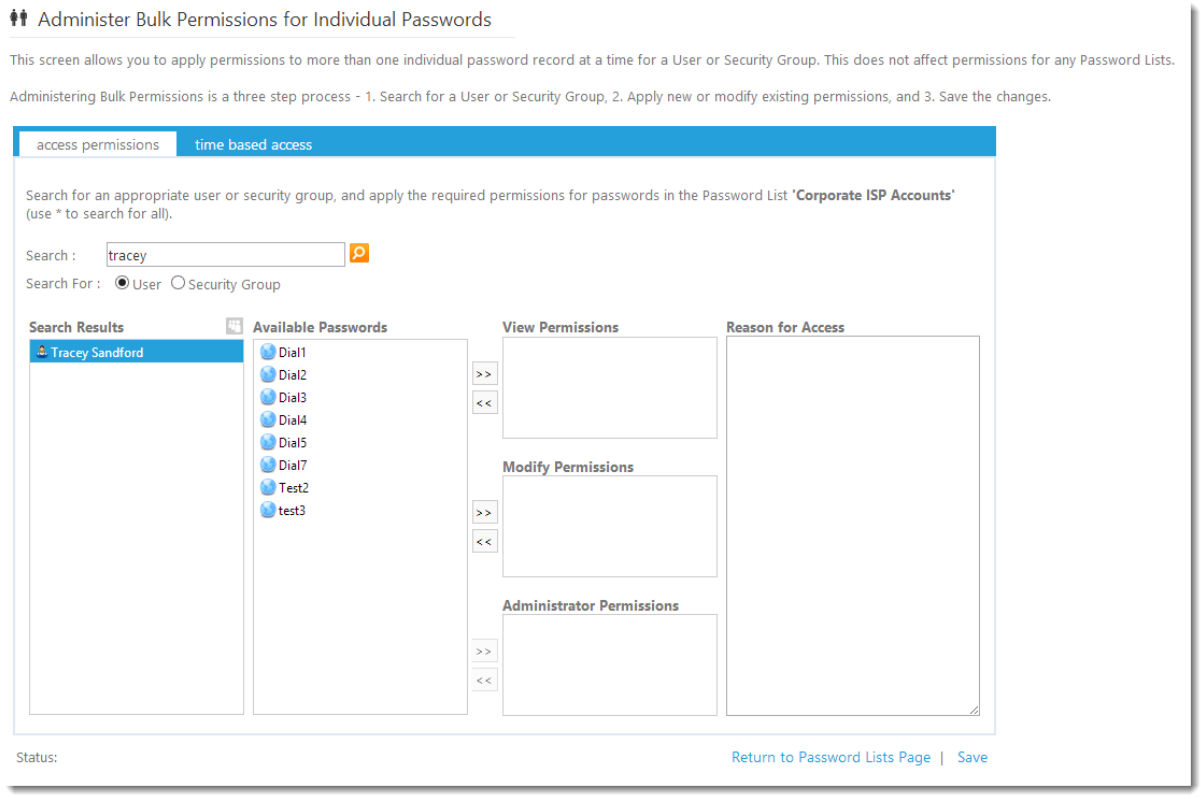
## Actions Menu - View Password List Permissions

By clicking on the 'View Password List Permissions' Action menu, you can view all permissions which are applied to the Password List. From here you can make any number of changes to permissions as required.

## Actions Menu - Bulk Permissions for Individual Passwords

By clicking on the 'Bulk Permissions for Individual Passwords' menu option in the 'Actions' drop-down menu, you will be able to apply permissions for a user account or security group to multiple individual password records at once.

© 2014 Click Studios (SA) Pty Ltd


Administer Bulk Permissions for Individual Passwords
This screen allows you to apply permissions to more than one individual password record at a time for a User or Security Group. This does not affect permissions for any Password Lists.
Administering Bulk Permissions is a three step process - 1. Search for a User or Security Group, 2. Apply new or modify existing permissions, and 3. Save the changes.
access permissions
time based access
Search for an appropriate user or security group, and apply the required permissions for passwords in the Password List 'Corporate ISP Accounts' (use * to search for all).
Search :
tracey
Search For : User Security Group
Search Results
Tracey Sandford
Available Passwords
Dial1
Dial2
Dial3
Dial4
Dial5
Dial7
Test2
test3
View Permissions
Modify Permissions
Administrator Permissions
Reason for Access
Status:
Return to Password Lists Page | Save

## Actions Menu - Convert to Private Password List

Under certain circumstances, you may want to change a Shared Password List into a Private one.

Warning: Please use this feature with caution, as it is an irreversible process once complete - you will need to restore a copy of your database if you wish to undo any changes with this feature.

In order to use this feature, you must first apply permissions to only the intended recipient of the Private Password List - meaning you must remove all Security Group permissions, and any other 'user account' based permissions why are not appropriate for a Private Password List. Once you have done this and select this feature, the following processes will occur:

- Delete any 'permission' records applied at the individual password record level
- Delete any 'Favorite' password records for the list
- Delete any linkages to Password List Templates
- If any users have the Password List set as their Default Home Page, then it will be changed to the 'Passwords Home' node in the Navigation Tree
- And finally it will marked the Password List as private

## Actions Menu - Delete Password List

By selecting the 'Delete Password List' menu option in the 'Actions' drop-down menu, you will be

© 2014 Click Studios (SA) Pty Ltd

given the opportunity to delete the selected Password List.

Warning: You are prompted twice to delete a Password List, or there is no Recycle Bin in the event you do delete one - so be sure you no longer require the passwords in this List. If you accidentally delete a Password List and still require it, you will need to ask your DBAs restored a copy of the database.

## Add Password List

By clicking on the 'Add Password Lists' button, you will be able to add a new Password List to Passwordstate.

Note: Please refer to the Passwordstate User Manual for detailed instructions on settings which can be applied to new Password Lists or Templates.

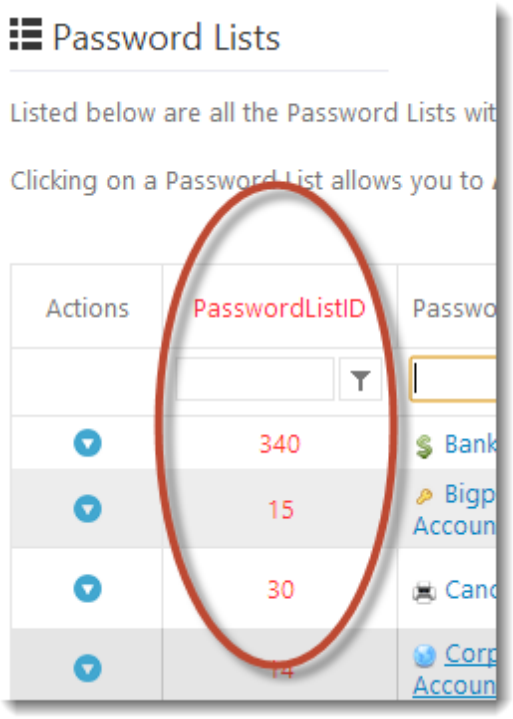
## Export

The Export button simply allows you to export the list of Password Lists to a csv file - no Passwords are exported, just basic information about the Password Lists themselves.

## Toggle ID Column Visibility

The Toggle ID Column Visibility button will either show or hide the PasswordListID value for each of the Password Lists. These PasswordListID values may be required if you are using the Passwordstate API, or the Bulk Password Import feature below.

© 2014 Click Studios (SA) Pty Ltd




## Perform Bulk Processing - Administer Bulk Permissions

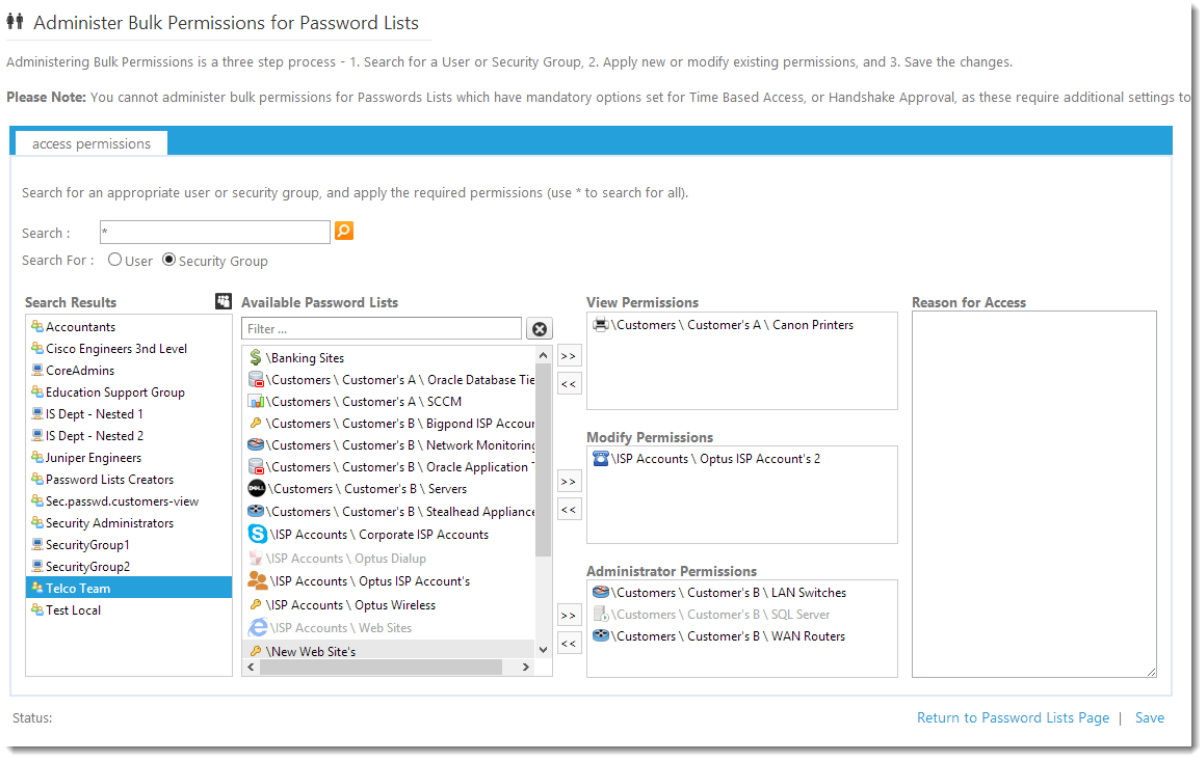
Administer Bulk Permissions allows you to apply new permissions, or remove permissions, for a user account or security group to multiple Password Lists at once.

After you have searched for a user account or security group, and then clicked on it, the 'Available Password Lists' listbox shows which Password Lists the user/security group does not have access to, and the 'View/Modify/Administrator Permissions' listbox shows what Password Lists the user/security group already has access to.

To apply new permissions, or remove existing permissions, simply move the Password Lists between the different listboxes using the various arrow buttons, then click on the Save button.

Note: You cannot manage permissions here for Password Lists which have mandatory options set for Time-Based Access, or Handshake approval.

© 2014 Click Studios (SA) Pty Ltd

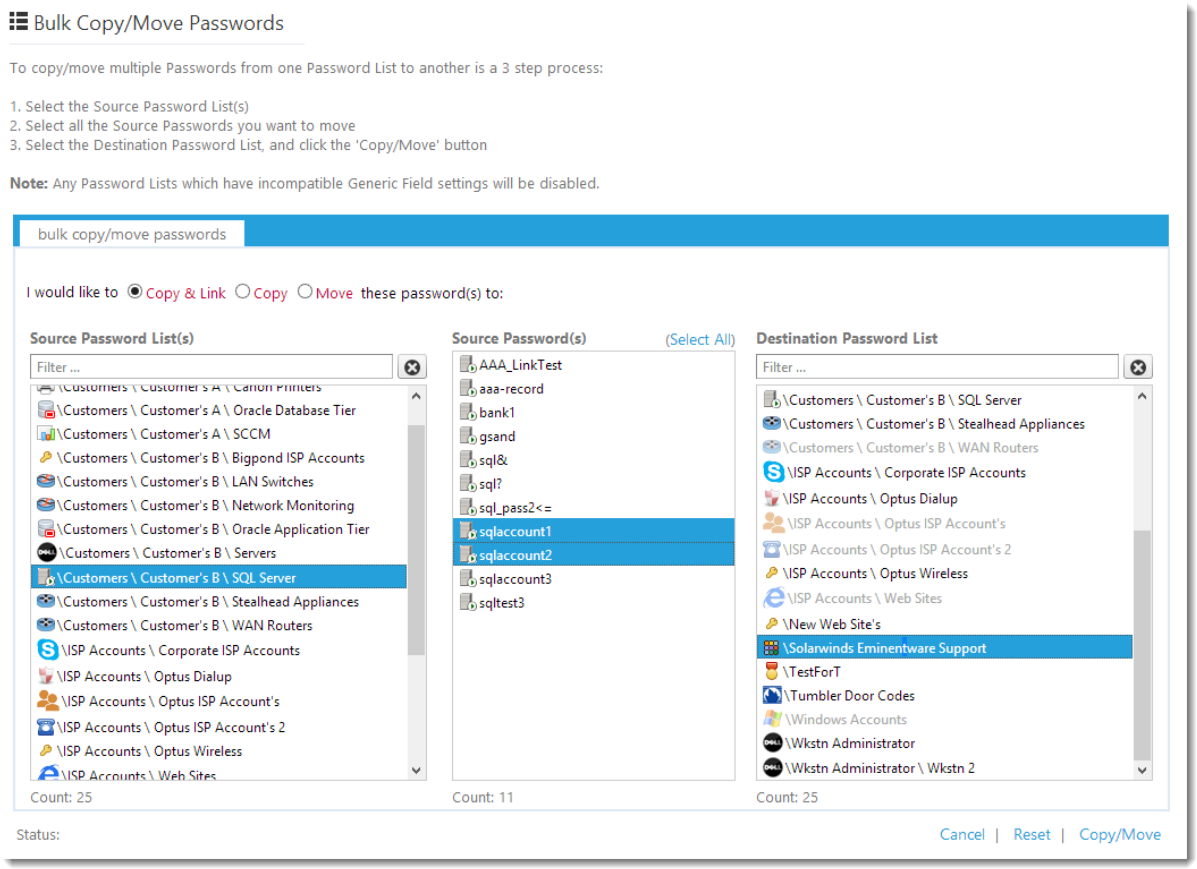

Administer Bulk Permissions for Password Lists
Administering Bulk Permissions is a three step process - 1. Search for a User or Security Group, 2. Apply new or modify existing permissions, and 3. Save the changes.
Please Note: You cannot administer bulk permissions for Passwords Lists which have mandatory options set for Time Based Access, or Handshake Approval, as these require additional settings to
access permissions
Search for an appropriate user or security group, and apply the required permissions (use * to search for all).
Search :
Search For : User Security Group
Search Results
Accountants
Cisco Engineers 3nd Level
CoreAdmins
Education Support Group
IS Dept - Nested 1
IS Dept - Nested 2
Juniper Engineers
Password Lists Creators
Sec.passwd.customers-view
Security Administrators
SecurityGroup1
SecurityGroup2
Telco Team
Test Local
Available Password Lists
Filter ...
\Banking Sites
\Customers \ Customer's A \ Oracle Database Tie
\Customers \ Customer's A \ SCCM
\Customers \ Customer's B \ Bigpond ISP Accour
\Customers \ Customer's B \ Network Monitorin
\Customers \ Customer's B \ Oracle Application
\Customers \ Customer's B \ Servers
\Customers \ Customer's B \ Stealhead Appliance
\ISP Accounts \ Corporate ISP Accounts
\ISP Accounts \ Optus Dialup
\ISP Accounts \ Optus ISP Account's
\ISP Accounts \ Optus Wireless
\ISP Accounts \ Web Sites
\New Web Site's
View Permissions
\Customers \ Customer's A \ Canon Printers
Modify Permissions
\ISP Accounts \ Optus ISP Account's 2
Administrator Permissions
\Customers \ Customer's B \ LAN Switches
\Customers \ Customer's B \ SQL Server
\Customers \ Customer's B \ WAN Routers
Reason for Access
Status:
Return to Password Lists Page | Save

## Perform Bulk Processing - Bulk Copy/Move Passwords

The Bulk Copy/Move Passwords feature allows you to Copy, Move or Copy & Link multiple passwords from multiple Password Lists to a different Password List at once - instead of doing one record at a time as users can do through the standard interface. This feature is useful if you are re-organizing your Password Lists, and need to move records around in mass.

Note: You can only copy/move records between Password Lists which have similar fields configured. If the fields are not compatible, then the destination Password List will be disabled, preventing you from copying/moving records to it.

© 2014 Click Studios (SA) Pty Ltd


Bulk Copy/Move Passwords
To copy/move multiple Passwords from one Password List to another is a 3 step process:
1. Select the Source Password List(s)
2. Select all the Source Passwords you want to move
3. Select the Destination Password List, and click the 'Copy/Move' button
Note: Any Password Lists which have incompatible Generic Field settings will be disabled.
bulk copy/move passwords
I would like to Copy & Link Copy Move these password(s) to:
Source Password List(s)
Source Password(s)
(Select All)
Destination Password List
Filter ...
\Customers \ Customer's A \ Oracle Database Tier
\Customers \ Customer's A \ SCCM
\Customers \ Customer's B \ Bigpond ISP Accounts
\Customers \ Customer's B \ LAN Switches
\Customers \ Customer's B \ Network Monitoring
\Customers \ Customer's B \ Oracle Application Tier
\Customers \ Customer's B \ Servers
\Customers \ Customer's B \ SQL Server
\Customers \ Customer's B \ Stealhead Appliances
\Customers \ Customer's B \ WAN Routers
\ISP Accounts \ Corporate ISP Accounts
\ISP Accounts \ Optus Dialup
\ISP Accounts \ Optus ISP Account's
\ISP Accounts \ Optus ISP Account's 2
\ISP Accounts \ Optus Wireless
Count: 25
AAA_LinkTest
aaa-record
bank1
gsand
sql&
sql?
sql_pass2<=
sqlaccount1
sqlaccount2
sqlaccount3
sqltest3
Count: 11
\Customers \ Customer's B \ SQL Server
\Customers \ Customer's B \ Stealhead Appliances
\Customers \ Customer's B \ WAN Routers
\ISP Accounts \ Corporate ISP Accounts
\ISP Accounts \ Optus Dialup
\ISP Accounts \ Optus ISP Account's
\ISP Accounts \ Optus ISP Account's 2
\ISP Accounts \ Optus Wireless
\ISP Accounts \ Web Sites
\New Web Site's
\Solarwinds Eminentware Support
\TestForT
\Tumbler Door Codes
\Windows Accounts
\Wkstn Administrator
\Wkstn Administrator \ Wkstn 2
Count: 25
Status:
Cancel | Reset | Copy/Move

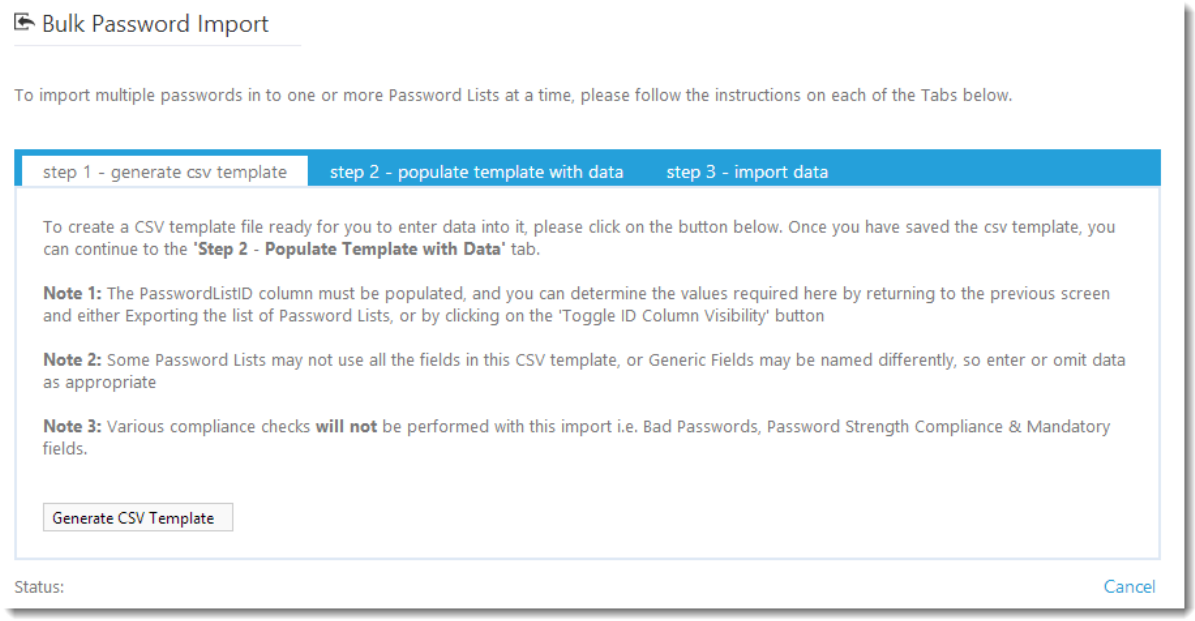
## Perform Bulk Processing - Bulk Password Import

The Bulk Password Import feature is useful when you are migrating data from another system, as it allows you to import multiple passwords records into multiple different Password Lists at once.

To import passwords in bulk is a 3 step process:

**Step 1 - Generate CSV Template**
By clicking on the 'Generate CSV Template' button you will be able to save an empty csv template file to your file system. It is this template you need to populate with data, ready for import.

© 2014 Click Studios (SA) Pty Ltd

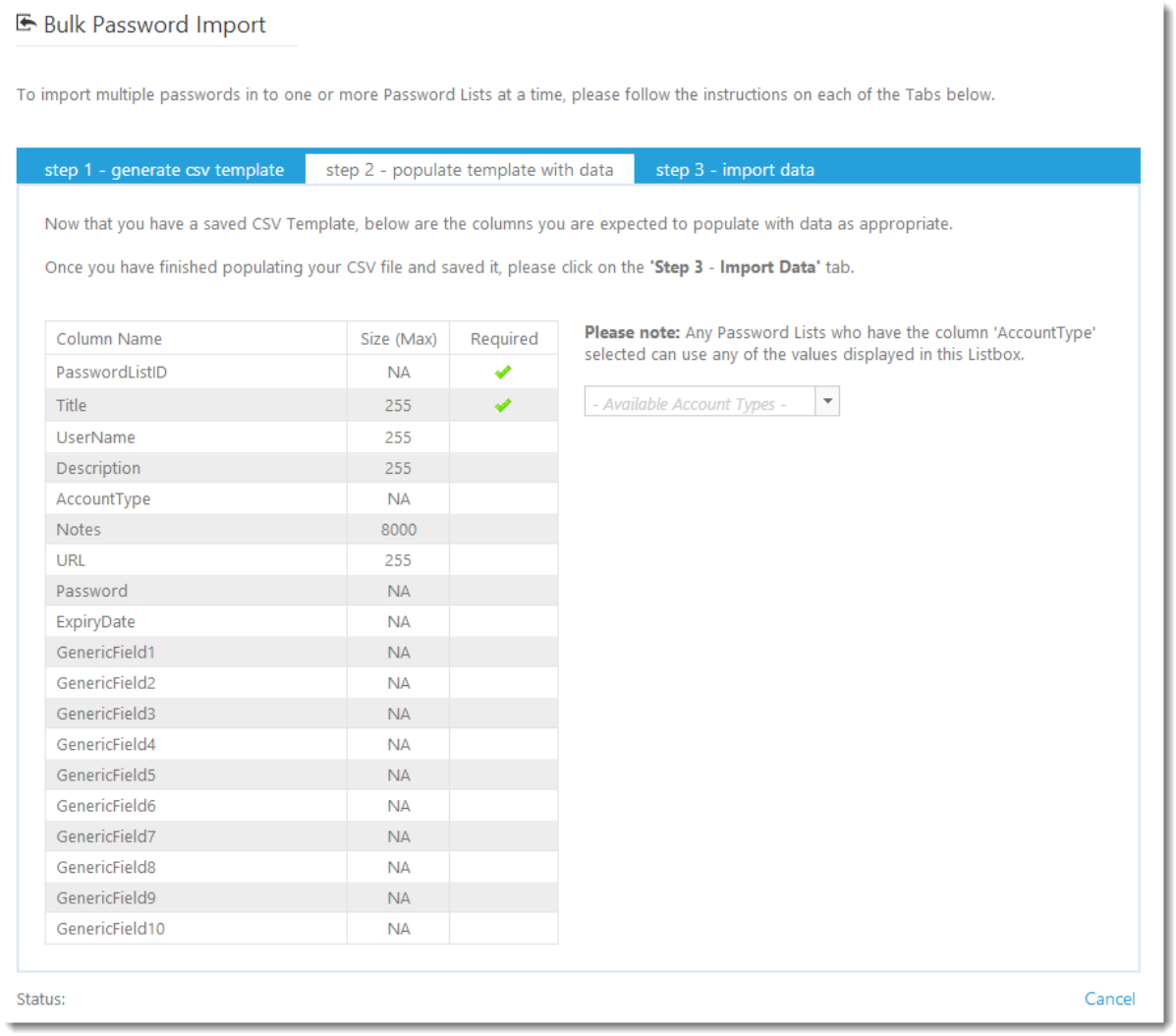

Bulk Password Import
To import multiple passwords in to one or more Password Lists at a time, please follow the instructions on each of the Tabs below.
step 1 - generate csv template
step 2 - populate template with data
step 3 - import data
To create a CSV template file ready for you to enter data into it, please click on the button below. Once you have saved the csv template, you can continue to the 'Step 2 - Populate Template with Data' tab.
Note 1: The PasswordListID column must be populated, and you can determine the values required here by returning to the previous screen and either Exporting the list of Password Lists, or by clicking on the 'Toggle ID Column Visibility' button
Note 2: Some Password Lists may not use all the fields in this CSV template, or Generic Fields may be named differently, so enter or omit data as appropriate
Note 3: Various compliance checks will not be performed with this import i.e. Bad Passwords, Password Strength Compliance & Mandatory fields.
Generate CSV Template
Status:
Cancel

**Step 2 - Populate Template with Data**
The screenshot below shows the fields which are populated in the csv template file, which fields are required, and the maximum size of any fields.

You will notice 10 Generic Fields in the csv template. By default, Password Lists are not configured to use any of the available Generic Fields, but it's possible they may have been configured to use them. Generally the Generic Fields are named differently, but those names cannot be shown in the csv template, as each Password List may have named them differently. You will need to ensure you populate the csv template file with the correct fields for each of the different Password Lists you are importing into.

Note 1: If a field is not 'Required', then you can leave it blank in the csv template
Note 2: The PasswordListID field is required so the import process knows which Password Lists to import the passwords into. The PasswordListID values can be determined by returning to the previous screen and either Exporting the list of Password Lists, or by clicking on the 'Toggle ID Column Visibility' button
Note 3: Various compliance checks will not be performed with this import i.e. Bad Passwords, Password Strength Compliance & Mandatory fields

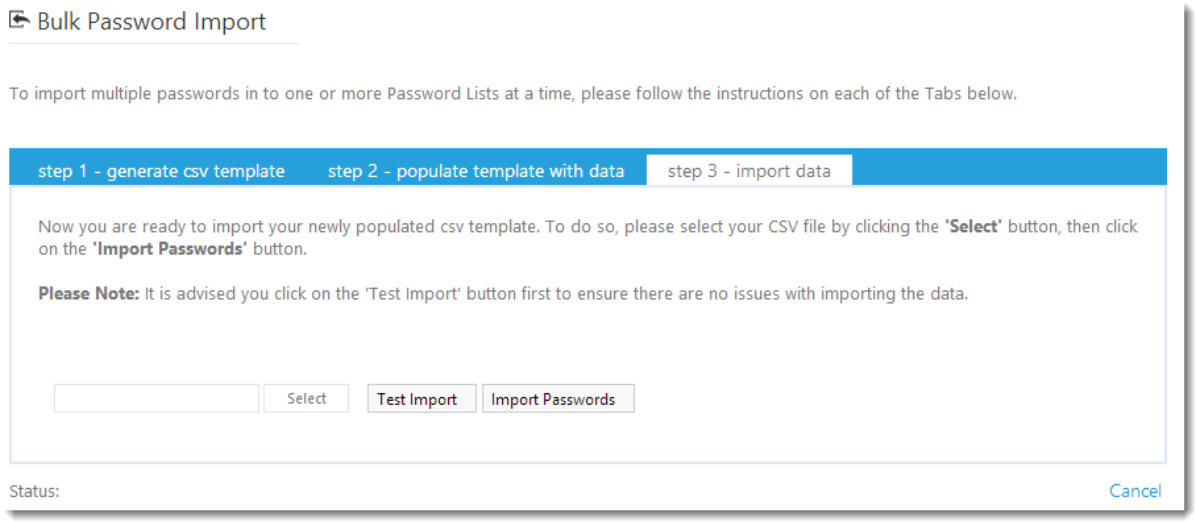
© 2014 Click Studios (SA) Pty Ltd




**Step 3 - Import Data**

Once you have populated the csv file with the required data, the 'Step 3' tab allows you to either test the import process, or perform the actual import. It is recommended you test the import process first, and any errors will be reported back to you, including the line number in the csv file so you're able to correct the data.

© 2014 Click Studios (SA) Pty Ltd

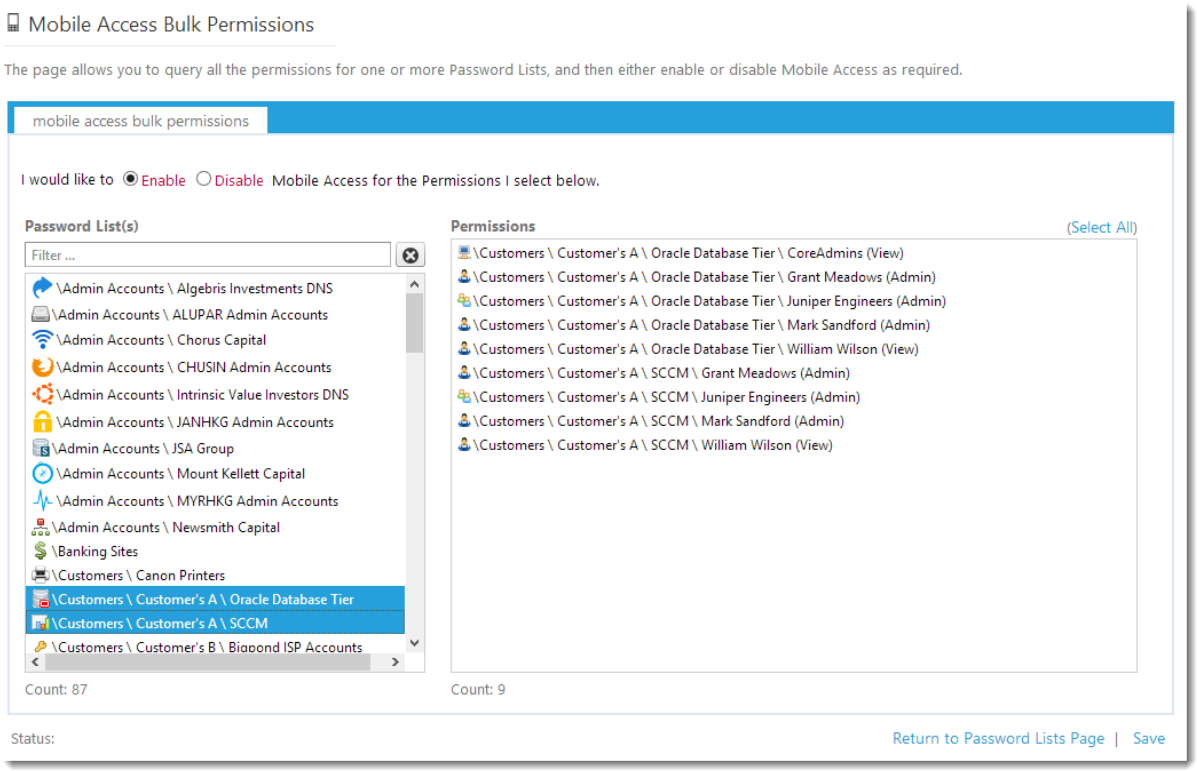

Bulk Password Import
To import multiple passwords in to one or more Password Lists at a time, please follow the instructions on each of the Tabs below.
step 1 - generate csv template
step 2 - populate template with data
step 3 - import data
Now you are ready to import your newly populated csv template. To do so, please select your CSV file by clicking the 'Select' button, then click on the 'Import Passwords' button.
Please Note: It is advised you click on the 'Test Import' button first to ensure there are no issues with importing the data.
Select
Test Import
Import Passwords
Status:
Cancel

## Perform Bulk Processing - Mobile Access Bulk Permissions

If you need to make many changes to Mobile Access Permissions at once, you can use the 'Mobile Access Bulk Permissions' feature.

This feature allows you to query all the permissions applied to one or more Password Lists, select the appropriate permissions (Guest, View, Modify or Admin), and then either enable or disable access for Mobile Clients.

© 2014 Click Studios (SA) Pty Ltd


Mobile Access Bulk Permissions
The page allows you to query all the permissions for one or more Password Lists, and then either enable or disable Mobile Access as required.
mobile access bulk permissions
I would like to Enable Disable Mobile Access for the Permissions I select below.
Password List(s)
Filter ...
\Admin Accounts \ Algebris Investments DNS
\Admin Accounts \ ALUPAR Admin Accounts
\Admin Accounts \ Chorus Capital
\Admin Accounts \ CHUSIN Admin Accounts
\Admin Accounts \ Intrinsic Value Investors DNS
\Admin Accounts \ JANHKG Admin Accounts
\Admin Accounts \ JSA Group
\Admin Accounts \ Mount Kellett Capital
\Admin Accounts \ MYRHKG Admin Accounts
\Admin Accounts \ Newsmith Capital
\Banking Sites
\Customers \ Canon Printers
\Customers \ Customer's A \ Oracle Database Tier
\Customers \ Customer's A \ SCCM
\Customers \ Customer's B \ Bigpond ISP Accounts
Count: 87
Permissions
(Select All)
\Customers \ Customer's A \ Oracle Database Tier \ CoreAdmins (View)
\Customers \ Customer's A \ Oracle Database Tier \ Grant Meadows (Admin)
\Customers \ Customer's A \ Oracle Database Tier \ Juniper Engineers (Admin)
\Customers \ Customer's A \ Oracle Database Tier \ Mark Sandford (Admin)
\Customers \ Customer's A \ Oracle Database Tier \ William Wilson (View)
\Customers \ Customer's A \ SCCM \ Grant Meadows (Admin)
\Customers \ Customer's A \ SCCM \ Juniper Engineers (Admin)
\Customers \ Customer's A \ SCCM \ Mark Sandford (Admin)
\Customers \ Customer's A \ SCCM \ William Wilson (View)
Count: 9
Status:
Return to Password Lists Page | Save

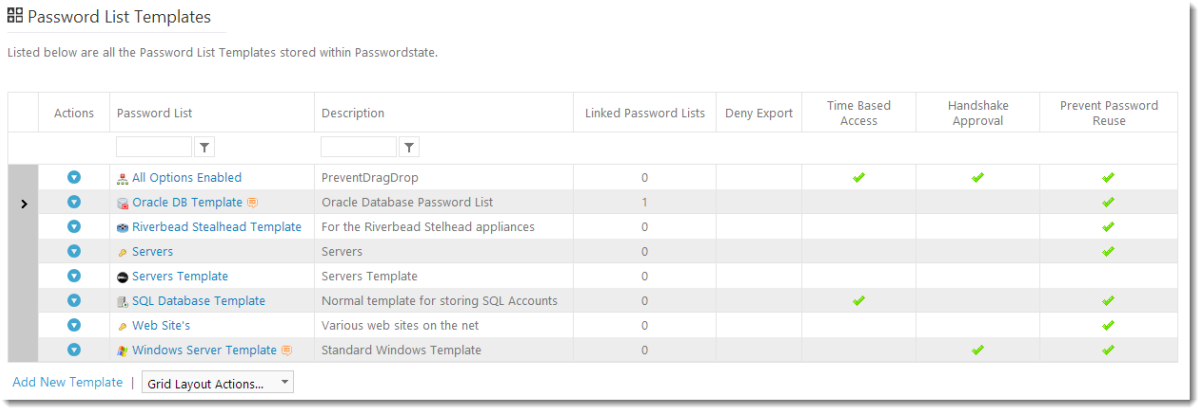
# 18 Password List Templates

Password List Templates can be used to apply consistency to settings for your Password Lists, and accessing the Templates from within the Administration area allows you to see all Templates created by all user. Templates can be used in the following way:

- You can apply a Template's settings as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings
- You can link Password Lists to a Template, and then manage all settings from the Template. When you do this, the majority of options for the Password List will be disabled when you chose to Edit Password List Details
- You can also apply permissions to a Template, and these permissions can be used for:
  - Allow other users to see the Templates via the 'Password List Templates' menu option
  - Allow other users to also modify the settings for the Template via the 'Password List Templates' menu option
  - Applying permissions to a Password List as needed (once off) when you add a new Password List, or edit an existing Password Lists' settings

Note: Permissions on a Template are not used when Linking Password Lists to a template - this can only be done when adding a new Password List, or editing the settings for an existing one.

© 2014 Click Studios (SA) Pty Ltd




## Adding and Editing Templates

Adding or editing templates in the Administration area is identical to the normal Password List Templates screens which standard user accounts have access to. For information on each of the settings which can be applied to a Template, please refer to the Passwordstate User Manual for creating Password Lists.

Caution: When editing a Template's settings when it is linked to other Password Lists, if you change any of the Field Types for any Generic Fields, these fields will have their data cleared/ blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

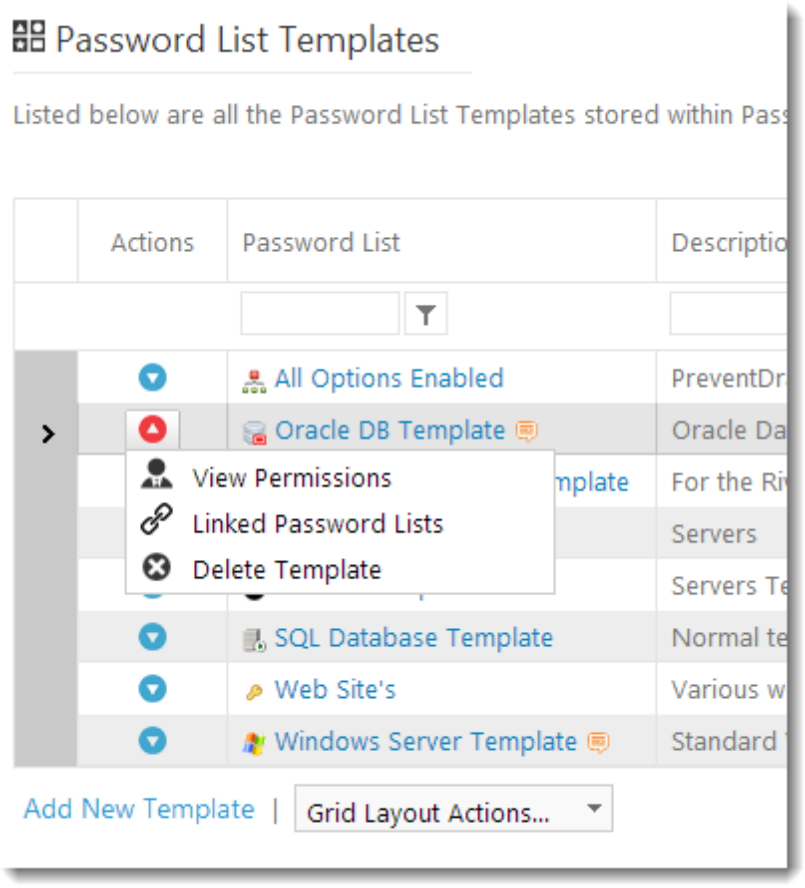
## Password List Template Actions

From the 'Actions' drop-down menu, you have various features available:

- View Permissions applied to the Template - this also allows you to add/update/delete permissions as required
- You can Link Password Lists to the Template
- You can delete the template

Note: If you delete a Template which is linked to one or more Password Lists, these Password Lists will bet set to use the Templates' settings as there were prior to you deleting the Template. You can then go ahead and modify the settings of the Password Lists as required.

© 2014 Click Studios (SA) Pty Ltd



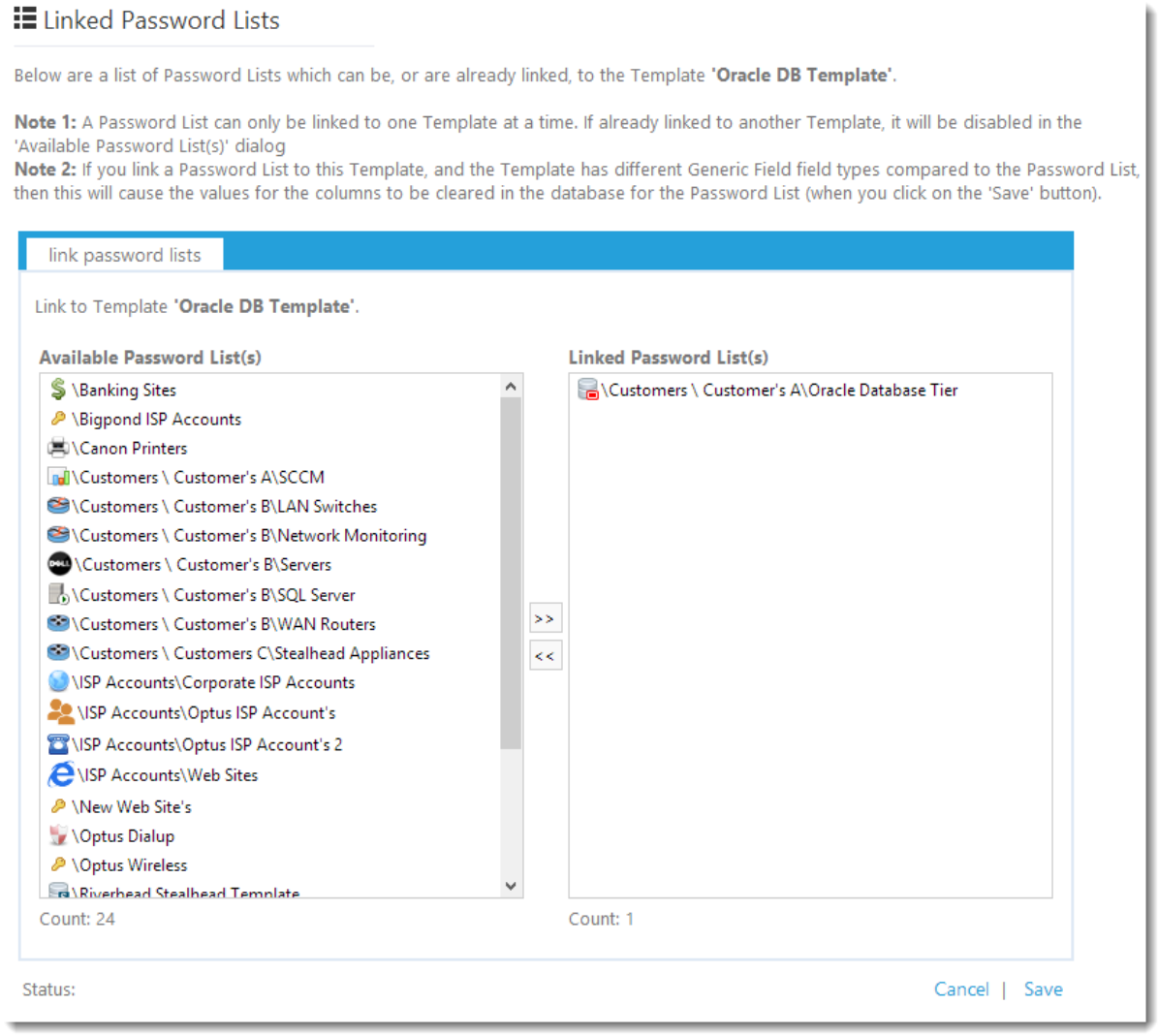

## Linked Password Lists

When you link one or more Password Lists to a Template, the majority of settings for the linked Password Lists are then managed via the Template - which the exception of the details on the API Key Tab.

Linking Password Lists to a Template is very simply process - move the Password List you want to link into the 'Linked Password List(s)' text box, and click on the 'Save' button.

Caution: When linking Password Lists to a Template for the first time, if the Password List has some Generic Fields specified which are different to any Generic Fields specified for the Template, these fields will have their data cleared/blanked in the database when you click on the 'Save' button. This is because the different Generic Field Field Types need to have their data treated differently. There are multiple warning messages within the Passwordstate as well for this, so please be aware.

© 2014 Click Studios (SA) Pty Ltd


Linked Password Lists
Below are a list of Password Lists which can be, or are already linked, to the Template 'Oracle DB Template'.
Note 1: A Password List can only be linked to one Template at a time. If already linked to another Template, it will be disabled in the 'Available Password List(s)' dialog
Note 2: If you link a Password List to this Template, and the Template has different Generic Field field types compared to the Password List, then this will cause the values for the columns to be cleared in the database for the Password List (when you click on the 'Save' button).
link password lists
Link to Template 'Oracle DB Template'.
Available Password List(s)
\Banking Sites
\Bigpond ISP Accounts
\Canon Printers
\Customers \ Customer's A\SCCM
\Customers \ Customer's B\LAN Switches
\Customers \ Customer's B\Network Monitoring
\Customers \ Customer's B\Servers
\Customers \ Customer's B\SQL Server
\Customers \ Customer's B\WAN Routers
\Customers \ Customers C\Stealhead Appliances
\ISP Accounts\Corporate ISP Accounts
\ISP Accounts\Optus ISP Account's
\ISP Accounts\Optus ISP Account's 2
\ISP Accounts\Web Sites
\New Web Site's
\Optus Dialup
\Optus Wireless
>>
<<
Linked Password List(s)
\Customers \ Customer's A\Oracle Database Tier
Count: 24
Count: 1
Status:
Cancel | Save

# 19 Password Strength Policies

Password Strength Policies are used as a set of rules for determining the strength of a Password. Once a policy is created, it can be applied to one or more Password Lists.

When adding or editing a Password Strength Policy, settings can be applied on 2 of the tabs, and there is 1 tab for testing the policy.

## Policy Settings Tab

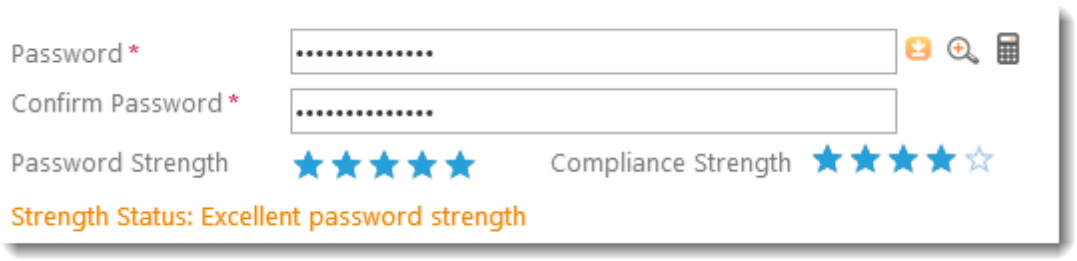
The Policy Settings Tab allows you to provide a name and description for the policy, plus the following settings:

- Minimum LowerCase Characters - specifies how many lowercase characters are required as a minimum (abcd, etc)
- Minimum UpperCase Characters - specifies how many uppercase characters are required as a

© 2014 Click Studios (SA) Pty Ltd

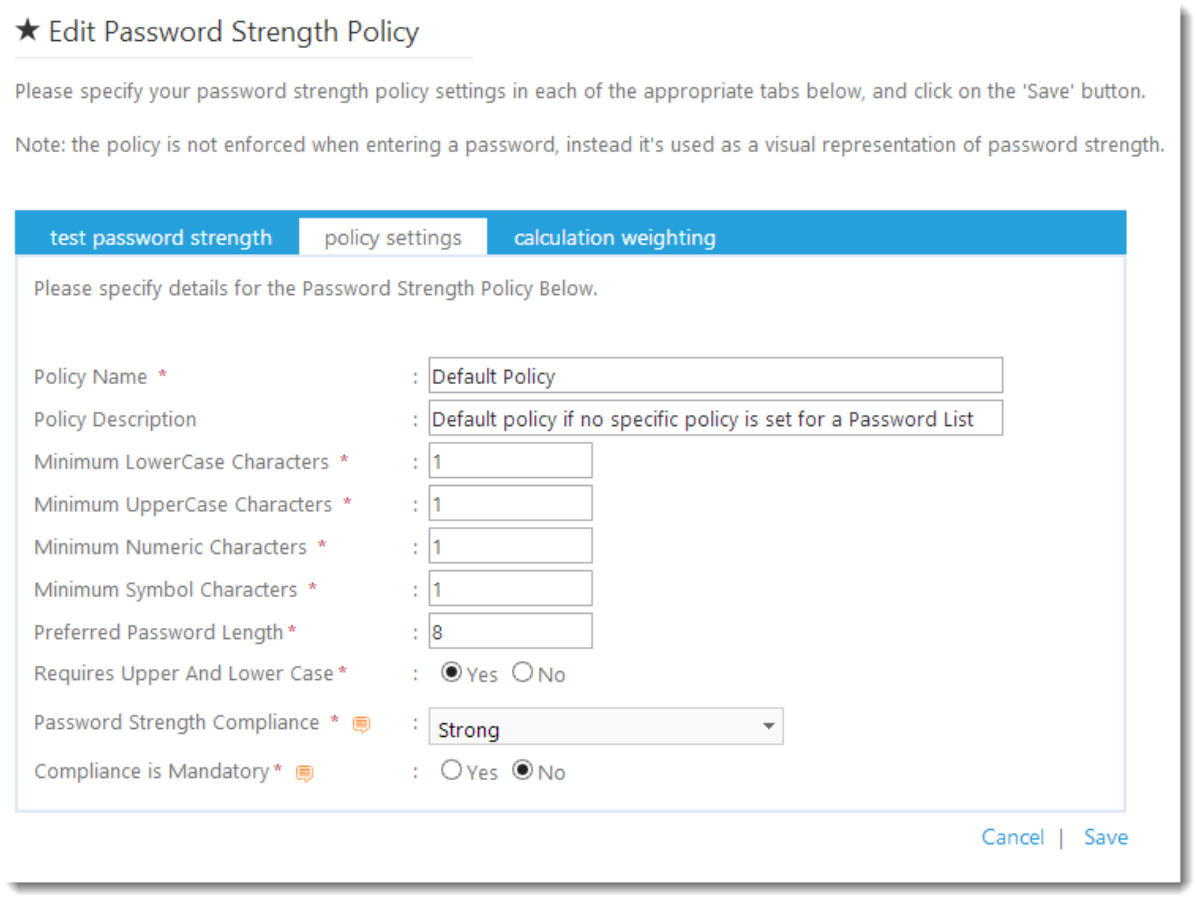
minimum (ABDCD, etc)

- Minimum Numeric Characters - specifies how many numeric characters are required as a minimum (1,2,3,etc)
- Minimum Symbol Characters - specifies how many symbol characters are required as a minimum (%@:!, etc)
- Preferred Password Length - specifies the minimum number of total characters the password should have
- Requires Upper And Lower Case - indicates if the passwords string must have both lower and uppercase characters
- Password Strength Compliance - indicates the desired Password Strength Complexity (Very Poor, Weak, Average, Strong or Excellent). With the following graphic when editing/adding a password, the 'Compliance Strength' indicator shows the user what password complexity is desired for the applied policy




- Compliance is Mandatory - if this option is set to Yes, the user will not be able to save the password record if the strength of the password they're creating does not meet the 'Password Strength Compliance' setting above

© 2014 Click Studios (SA) Pty Ltd

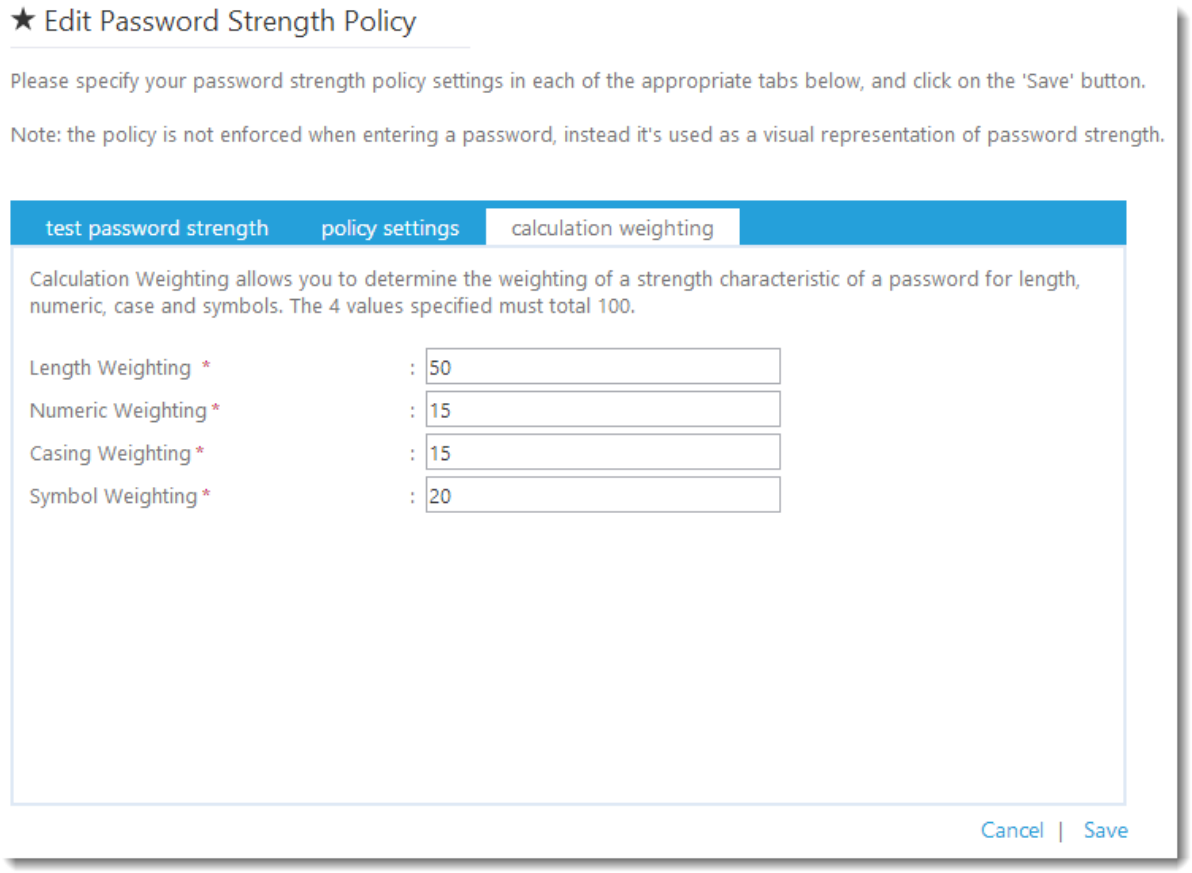

★ Edit Password Strength Policy
Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.
Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.
test password strength
policy settings
calculation weighting
Please specify details for the Password Strength Policy Below.
Policy Name *
Default Policy
Policy Description
Default policy if no specific policy is set for a Password List
Minimum LowerCase Characters *
1
Minimum UpperCase Characters *
1
Minimum Numeric Characters *
1
Minimum Symbol Characters *
1
Preferred Password Length *
8
Requires Upper And Lower Case *
Yes
No
Password Strength Compliance *
Strong
Compliance is Mandatory *
Yes
No
Cancel | Save

## Calculated Weighting Tab

The Calculated Weighting Tab allows you to specify the weighting of a strength characteristic of a password for length, numeric, case and symbols. The higher the weighting, the more important the category is deemed to be.

Note: The 4 values specified must total 100.

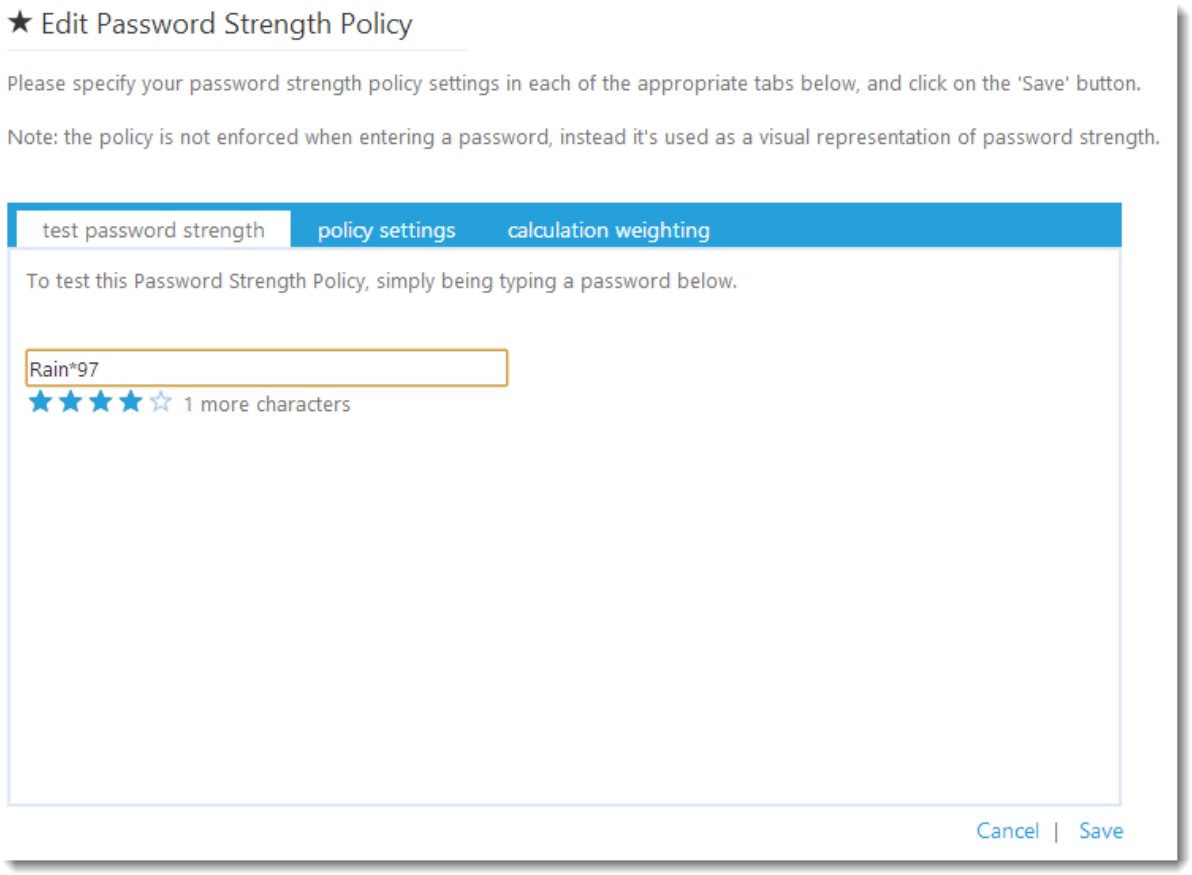
© 2014 Click Studios (SA) Pty Ltd


Edit Password Strength Policy
Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.
Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.
test password strength
policy settings
calculation weighting
Calculation Weighting allows you to determine the weighting of a strength characteristic of a password for length, numeric, case and symbols. The 4 values specified must total 100.
Length Weighting *
: 50
Numeric Weighting *
: 15
Casing Weighting *
: 15
Symbol Weighting *
: 20
Cancel | Save

## Test Password Strength Tab

The Test Password Strength Tab allows you to test the policy settings you've specified on the other two tabs, and shows you a graphical representation of the strength of the password you type, based on the policy settings you've specified.

© 2014 Click Studios (SA) Pty Ltd


★ Edit Password Strength Policy
Please specify your password strength policy settings in each of the appropriate tabs below, and click on the 'Save' button.
Note: the policy is not enforced when entering a password, instead it's used as a visual representation of password strength.
test password strength
policy settings
calculation weighting
To test this Password Strength Policy, simply being typing a password below.
Rain*97
1 more characters
Cancel | Save

# 20 Reporting

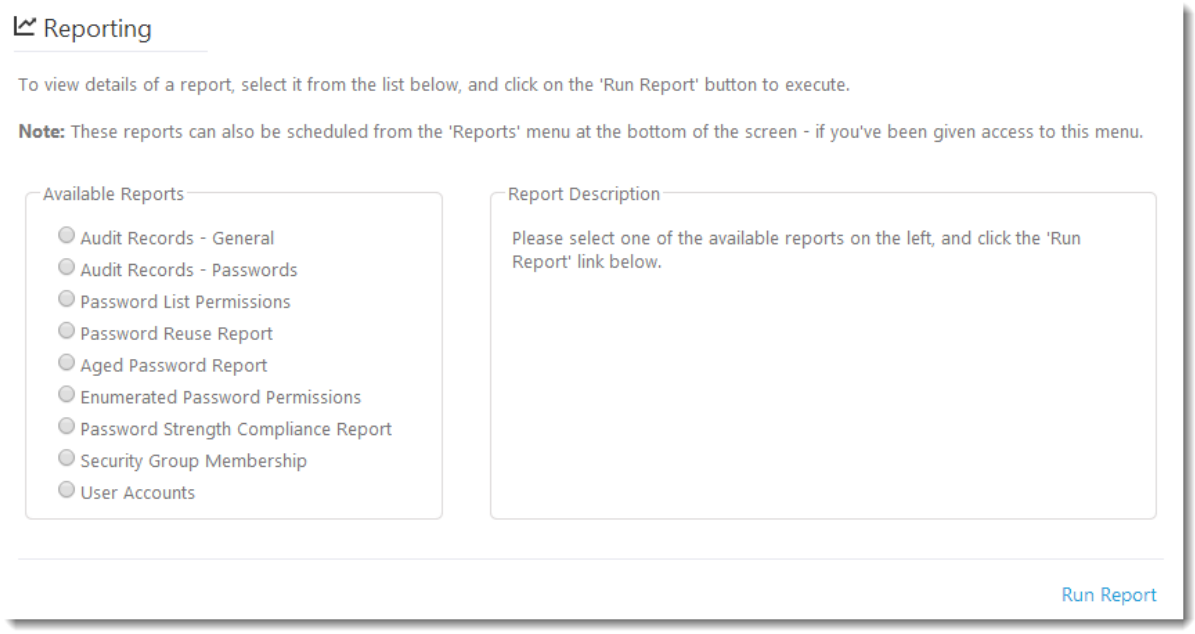
The Reporting feature allows you to run the following reports, which will be exported to csv files for further analysis if required:

- Audit Records (General) - exports a sorted list of all general audit records, not specific to Passwords or Password Lists. Please note this could be a large CSV file, so may take some time to generate
- Audit Records (Passwords) - exports a sorted list of all audit records specific to Passwords and Password Lists. Please note this could be a large CSV file, so may take some time to generate
- Password List Permissions - exports a sorted list of permissions for all Password Lists, and any permissions applied to individual passwords. Note: if the Title field is populated in this report, then it means the permissions have been applied to the individual password record
- Password Reuse Report - exports a list of records where the same password have been used more than once.
- Aged Password Report - exports a list of each individual password record, showing the last time any activity occurred for each record (excludes Private Password Lists).
- Enumerated Password Permissions - exports a sorted list of permissions for every individual password recorded in Passwordstate (excluding Private Password Lists). It will show

© 2014 Click Studios (SA) Pty Ltd

permissions based on users, and will enumerate any Security Groups into User Account details
- Password Strength Compliance Report - exports a sorted list of all Password Lists, the strength of each password, and whether or not the Password Strength is compliant or not
- Security Group Membership - exports a sorted list of Security Groups within Passwordstate, and their User Accounts membership
- User Accounts - exports a sorted list of User Accounts within Passwordstate

Note: No password values are exported in any of the reports on this screen.


Reporting
To view details of a report, select it from the list below, and click on the 'Run Report' button to execute.
Note: These reports can also be scheduled from the 'Reports' menu at the bottom of the screen - if you've been given access to this menu.
Available Reports
Audit Records - General
Audit Records - Passwords
Password List Permissions
Password Reuse Report
Aged Password Report
Enumerated Password Permissions
Password Strength Compliance Report
Security Group Membership
User Accounts
Report Description
Please select one of the available reports on the left, and click the 'Run Report' link below.
Run Report

# 21 Security Administrators

The 'Security Administrator' role in Passwordstate provides access to one or more features in the Administration area. If a user's account is not set up as a Security Administrator, the Administration menu on the bottom horizontal menu will not be visible to them.

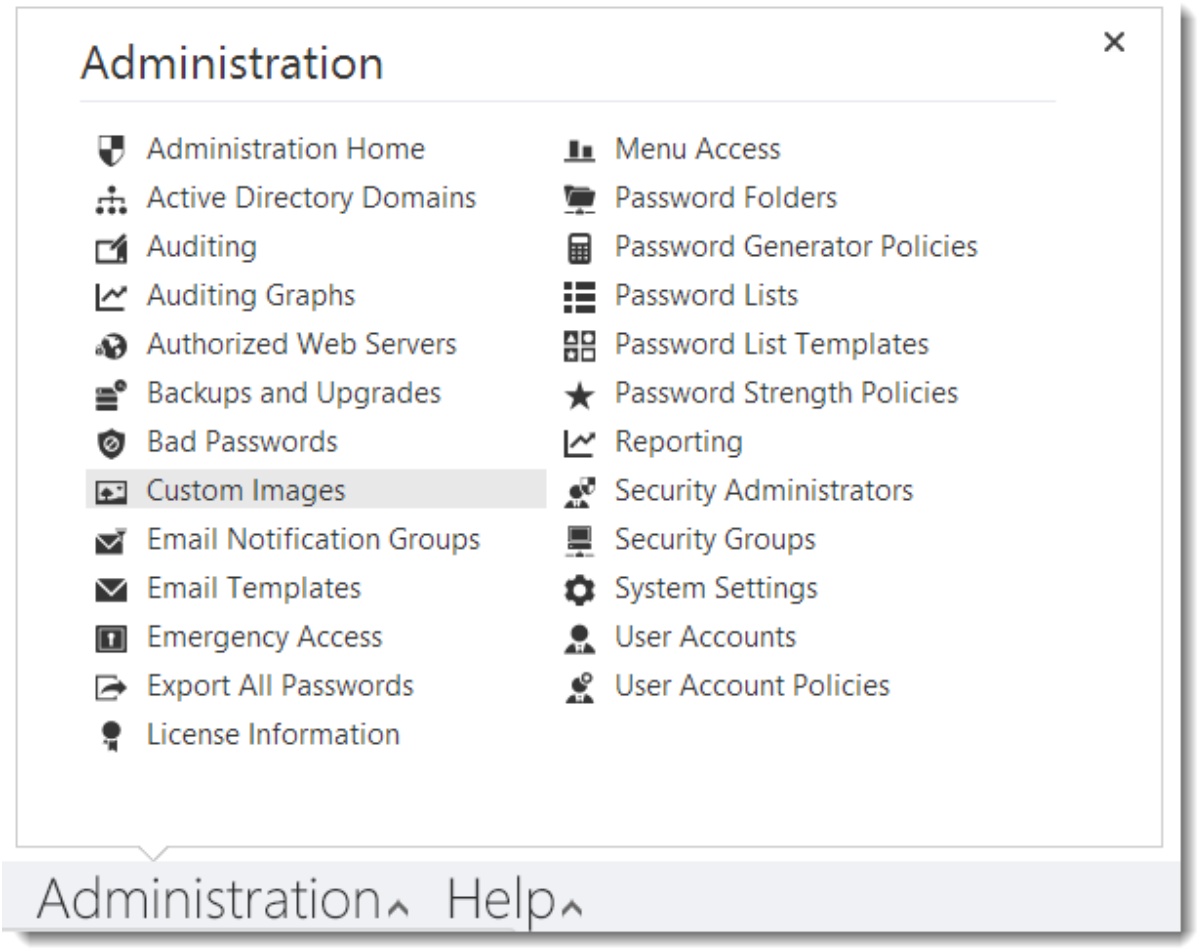
There are 15 different types of roles a Security Administrator account can be configured for, with each role providing access to various screens/features in the Administration area. The roles are:

| Role | Screen/Feature Access |
|---|---|
| Active Directory Domains | Active Directory Domains |
| Auditing | Auditing & Auditing Graphs |
| Bad Passwords | Bad Passwords |
| Email Templates | Email Notification Groups & Email Templates |
| Emergency Access | Emergency Access |
| Export All Passwords | Export All Passwords |
| Licensing | License Information |
| Password Generator | Password Generator Policies |

© 2014 Click Studios (SA) Pty Ltd

| | |
|---|---|
| Password Lists | Custom Images, Password Folders, Password Lists & Password List Templates |
| Password Strength Policy | Password Strength Policies |
| Reporting | Reporting |
| Security Administrators | Security Administrators |
| Security Groups | Security Groups |
| System Settings | Authorized Web Servers, Backups and Upgrades, Menu Access & System Settings |
| User Accounts | User Accounts & User Account Policies |

If you deselect one or more of the Security Administrator roles for a user, the corresponding menu item will be disabled for the Administration menu, as per the following graphic.




# 22 Security Groups

Security Groups allows you to manage either local security groups created within Passwordstate, or Active Directory security groups. These groups can then be used for applying permissions to Password Lists, or to give/deny access to various features.

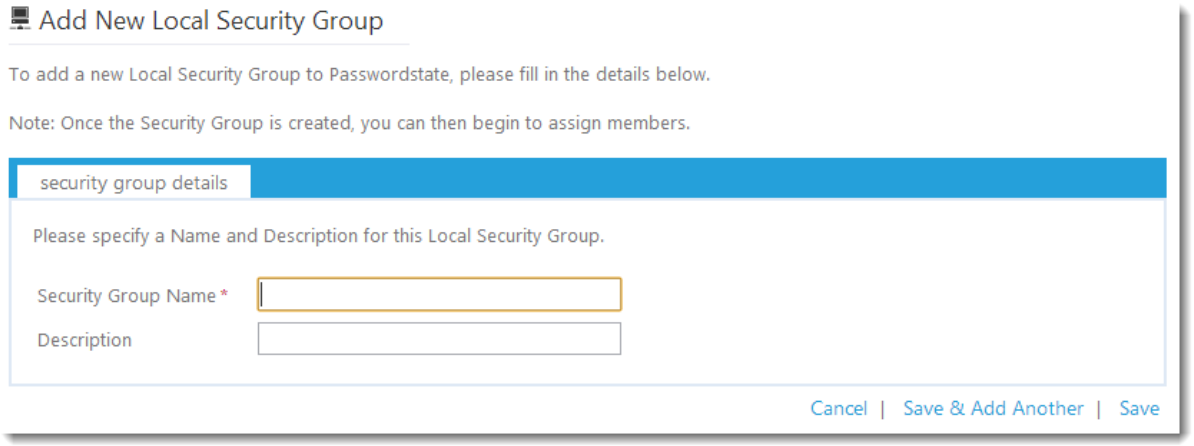
© 2014 Click Studios (SA) Pty Ltd

On the Security Groups screen, you have the following features available:

## Add Local Security Group

Allows you to add a "local" security group to Passwordstate, which you can then assign one or more user accounts to the security group.

Note: Once you have added the local security group, you can assign user account membership by selecting the 'Manage Members' menu item from the appropriate Actions menu


Add New Local Security Group
To add a new Local Security Group to Passwordstate, please fill in the details below.
Note: Once the Security Group is created, you can then begin to assign members.
security group details
Please specify a Name and Description for this Local Security Group.
Security Group Name *
Description
Cancel | Save & Add Another | Save

## Add Active Directory Security Group

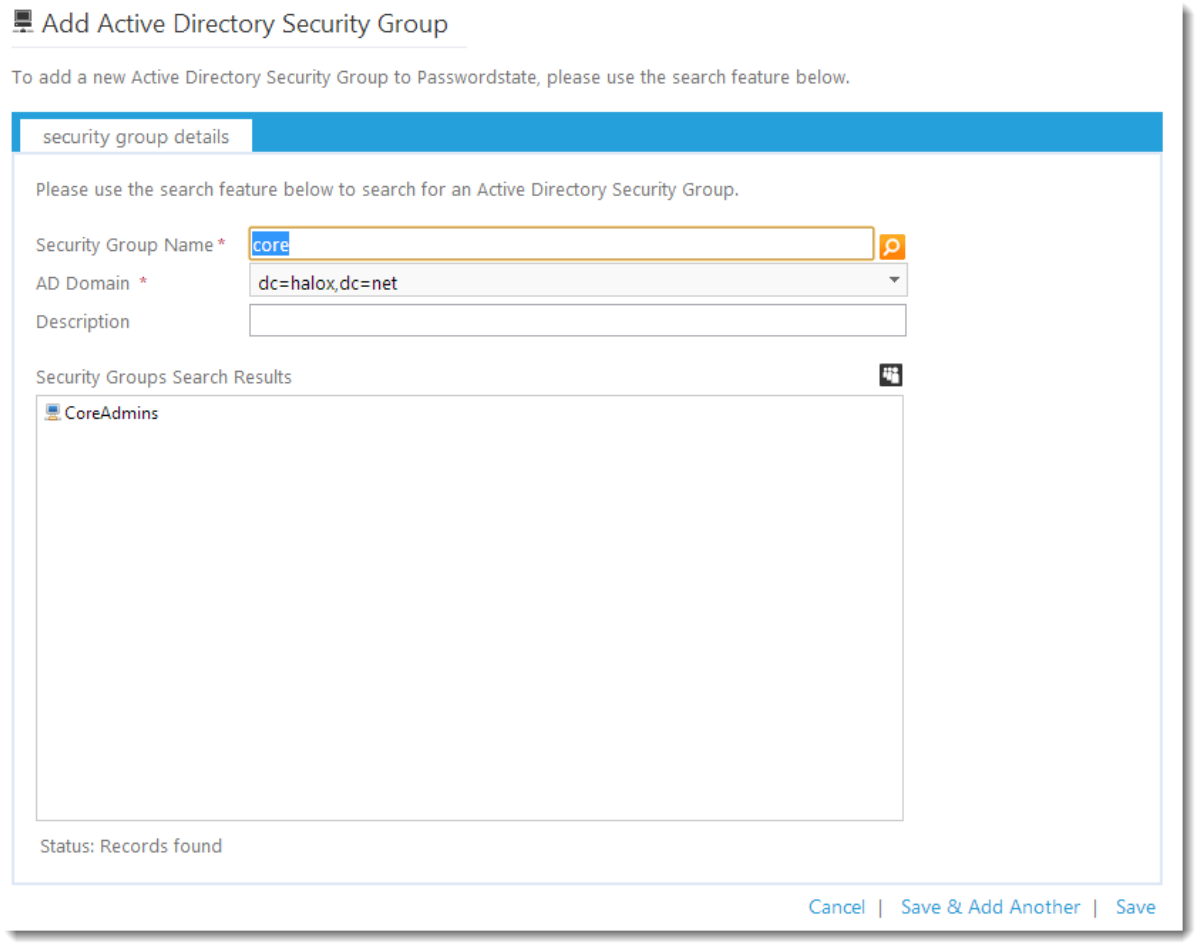
To add an Active Directory Security Group, you simply need to search for the group you require, then click on the appropriate Save button.

Note 1: The Active Directory Managed Service Account which you specify on the screen System Settings -> Active Directory Options Tab is what's used to query Active Directory, so this account will need read access at a minimum

Note 2: When you add a security group, if the user account does not already exist in Passwordstate (on the User Accounts screen), there is on option on the screen Administration -> System Settings -> Active Directory Options Tab which allows you to also automatically add the user account

Note 3: If you have issues querying Active Directory, please see the section 'Active Directory Lookup Permissions' below

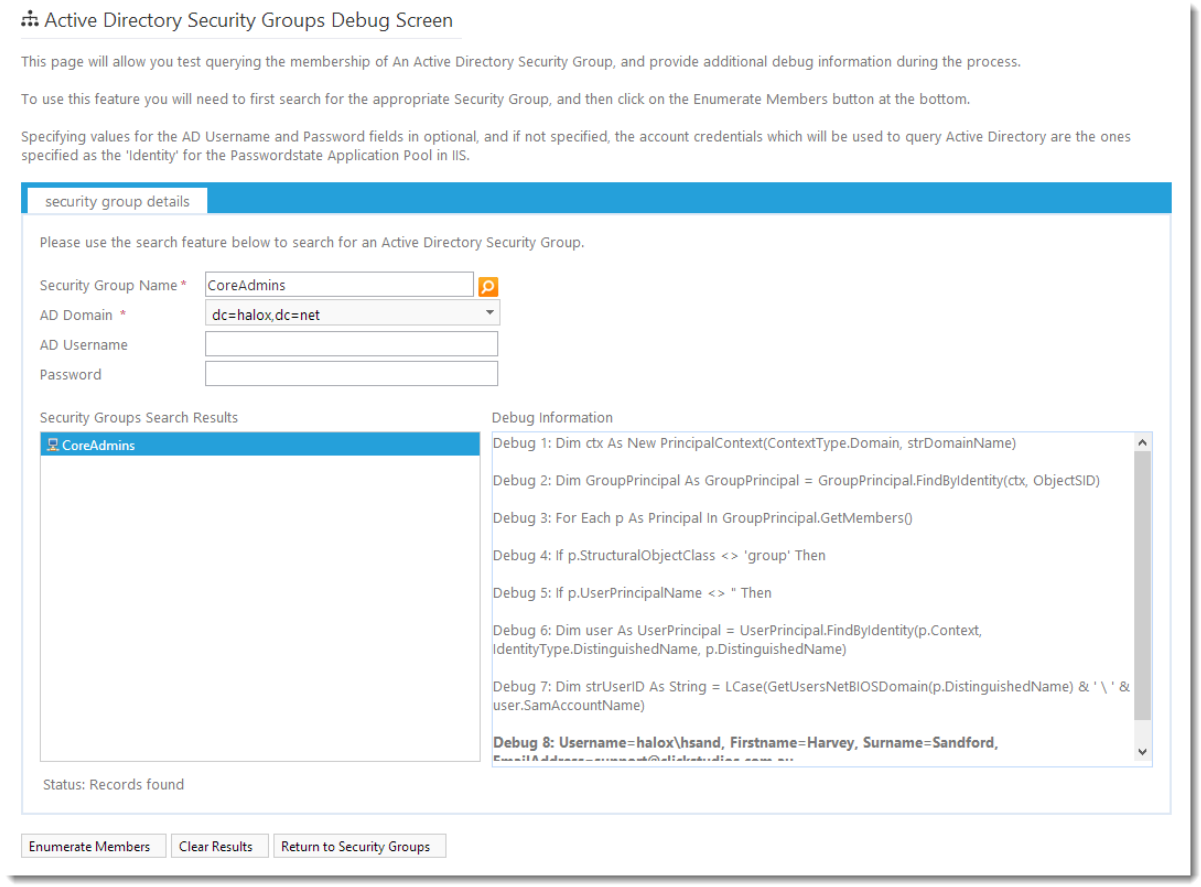
© 2014 Click Studios (SA) Pty Ltd


Add Active Directory Security Group
To add a new Active Directory Security Group to Passwordstate, please use the search feature below.
security group details
Please use the search feature below to search for an Active Directory Security Group.
Security Group Name *
core
AD Domain *
dc=halox,dc=net
Description
Security Groups Search Results
CoreAdmins
Status: Records found
Cancel | Save & Add Another | Save

## Debug Security Group Membership

In the event you are having some issue synchronizing the membership of an Active Directory Security Group, the 'Debug Security Group Membership' screen allows you to query the members of the security groups, and provide some additional debug information which may be useful for determine the cause of the issue.

© 2014 Click Studios (SA) Pty Ltd


Active Directory Security Groups Debug Screen
This page will allow you test querying the membership of An Active Directory Security Group, and provide additional debug information during the process.
To use this feature you will need to first search for the appropriate Security Group, and then click on the Enumerate Members button at the bottom.
Specifying values for the AD Username and Password fields in optional, and if not specified, the account credentials which will be used to query Active Directory are the ones specified as the 'Identity' for the Passwordstate Application Pool in IIS.
security group details
Please use the search feature below to search for an Active Directory Security Group.
Security Group Name *
CoreAdmins
AD Domain *
dc=halox,dc=net
AD Username
Password
Security Groups Search Results
CoreAdmins
Debug Information
Debug 1: Dim ctx As New PrincipalContext(ContextType.Domain, strDomainName)
Debug 2: Dim GroupPrincipal As GroupPrincipal = GroupPrincipal.FindByIdentity(ctx, ObjectSID)
Debug 3: For Each p As Principal In GroupPrincipal.GetMembers()
Debug 4: If p.StructuralObjectClass <> 'group' Then
Debug 5: If p.UserPrincipalName <> '' Then
Debug 6: Dim user As UserPrincipal = UserPrincipal.FindByIdentity(p.Context, IdentityType.DistinguishedName, p.DistinguishedName)
Debug 7: Dim strUserID As String = LCase(GetUsersNetBIOSDomain(p.DistinguishedName) & '\' & user.SamAccountName)
Debug 8: Username=halox\hsand, Firstname=Harvey, Surname=Sandford,
Status: Records found
Enumerate Members
Clear Results
Return to Security Groups

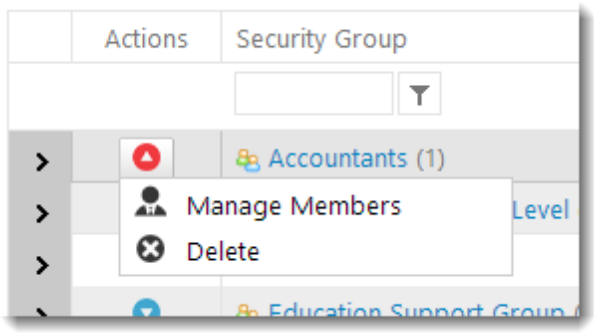
## Local Security Group Actions Menu

Once you have created a Local Security Group, the 'Actions' drop-down menu has two features you can use:

- Manage Members - allows you to add or remove members from the security group
- Delete - delete the security group from Passwordstate. This does not delete any user accounts, only the security group itself

Note: If the Security Group has been used to apply permissions anywhere within Passwordstate, removing members from the security group, or deleting the Security Group itself, will removes one or more user's access

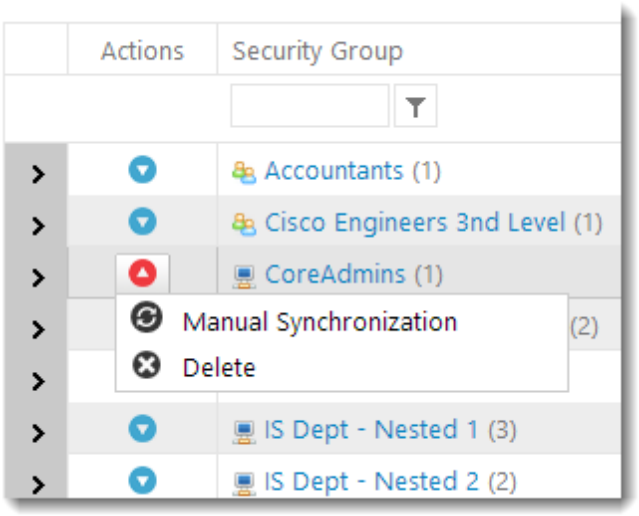
© 2014 Click Studios (SA) Pty Ltd




## Active Directory Security Group Actions Menu

Once you have add a new Active Directory Security Group, the 'Actions' drop-down menu has two features you can use:

- Manual Synchronization - synchronization membership of an Active Directory Security Group can be done in one of 3 ways:
  - When you first add an AD Security Group to Passwordstate
  - The Passwordstate Windows Service can perform the synchronization on the schedule you have specified on the screen Administration - > System Settings -> Active Directory Options Tab
  - Or by clicking the 'Manual Synchronization' menu item
- Delete - delete the security group from Passwordstate. This does not delete any user accounts in Passwordstate, and does not touch your Active Directory environment in any way




## Clone Security Group Permissions

It's possible to clone the permissions from one Security Group to another using the 'Clone Permissions' feature.

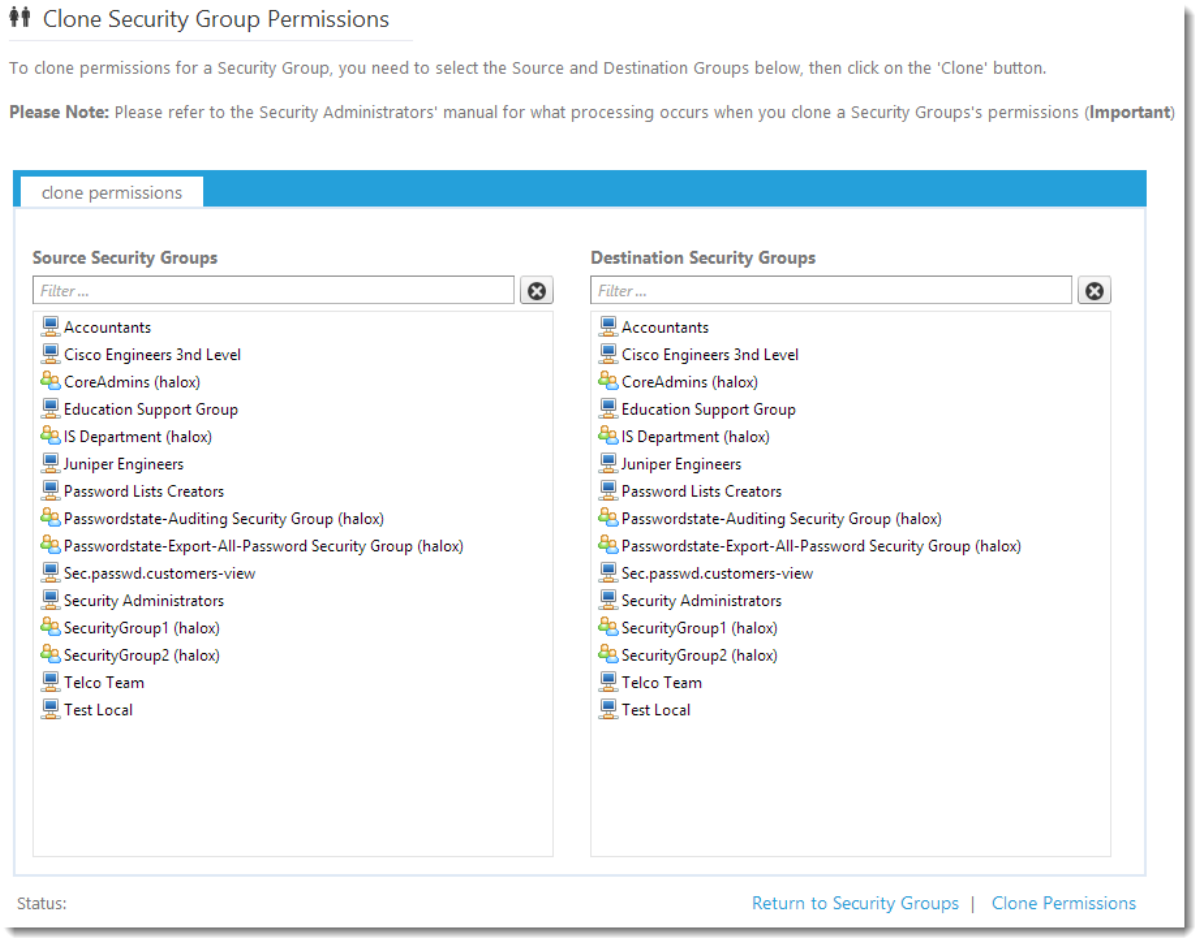
© 2014 Click Studios (SA) Pty Ltd

Note 1: When cloning occurs, the Destination Security Group's permissions are first removed – otherwise duplication would occur

Note 2: Security Group Memberships will not be cloned with this process, as you need to manage these memberships yourself - either manually for Local Security Groups, or by letting the AD synchronization work for AD groups.

During the cloning process, the following types of permissions will be cloned:

- Any memberships to Email Notification Groups
- Any of the 'Features' permissions for what menus the user is allowed access to at the bottom of the screen
- Any permissions to Password Lists (auditing records are added)
- Any Password Permissions (auditing records are added)
- Any permissions to Password Lists Templates (auditing records are added)
- Any Security Admin Roles (auditing records are added)
- Any User Account Policy permissions




© 2014 Click Studios (SA) Pty Ltd

# 23 System Settings

System Settings are used to specify any number of system wide settings in Passwordstate, which can affect the majority of users within the system.

| | |
|---|---|
| Miscellaneous Tab | Various settings which don't fall into any other of the 'Tab' categories |
| Password List Options Tab | Settings which are specific to Password Lists |
| Password Options Tab | Settings which are specific to individual password records |
| Email Alerts & Options Tab | Email Server settings, and multiple options for various email notifications |
| Proxy & Syslog Servers Tab | Specify proxy settings or syslog settings for Passwordstate to use |
| Active Directory Options Tab | Various settings for synchronizing Active Directory user accounts, security groups, and password synchronization with Active Directory |
| Authentication Options Tab | Various options and settings for authenticating to the Passwordstate web site |
| Password Synchronization Options | Specify settings and permissions for synchronizing passwords with Active Directory or Windows Servers |
| Mobile Access Options | Specify various system wide settings for the Mobile Access client |
| User Acceptance Policy Tab | Specify a popup 'User Acceptance Policy' which users must read when they access the Passwordstate web site |
| Check for Updates Tab | Specify how frequently Passwordstate should check for new versions |
| Branding Tab | Specify your own Logos and Page Titles to use on various screens and dialogs |
| High Availability Options Tab | Specify how frequently the High Availability instance of Passwordstate should check for new/update Custom Images and Logos, and write these to disk |
| Allowed IP Ranges Tab | Specify which IP Addresses or IP Address Ranges are allowed to access the Passwordstate web site or API |
| API Key Tab | Specify a System Wide API Key which can be used for various API calls |

## 23.1 Miscellaneous Tab

The Miscellaneous Tab has multiple settings which don't necessarily apply to any of the other Tabs.

### Default Locale (Date Format)

Applies date formatting rules to any date fields you see in Passwordstate. If users are located in a different region to what is set system wide, they can specify their own date format as part of their 'Preferences'.

© 2014 Click Studios (SA) Pty Ltd

## Inactivity Time Out (mins)

Allows you to specify the period in which users will be automatically logged out of Passwordstate if their session is inactive.

## If Audit records in the database are detected as being tampered with, send email reports at

The Passwordstate Windows Service monitors the state of the Auditing data in the database, and if it detects any modifications to data directly in the database, it can alert Security Administrators via an email. This setting allows you to specify what time on the day you would like to receive that notification.

## Specify the Base URL used in any emails generated by Passwordstate

This URL field is used as hyperlinks in any emails generated from Passwordstate.

## Force the use of an SSL Certificate (HTTPS)

When set to Yes, if the user types HTTP into the browser address bar, they will be redirected to HTTPS - which securely encrypts all traffic between the user's browser and the web site. The API will return a 403 Forbidden message if HTTPS is not used.

## Show Password List Auditing data to users with the following permissions

Beneath each Password List grid you see on the Password screens, there is a 'Recent Activity' grid. This data in the 'Recent Activity' grid is all auditing data specify to the Password List you are viewing. You can choose to hide this grid be deselecting the relevant role for this setting - this will also remove the Password List from the 'Auditing' section that users have access to.

## When expanding/collapsing nodes in the Passwords Navigation Tree, show a loading animation icon when the count of nodes in the tree is greater than

If you have many Password Lists and Folders visible in the Navigation Tree for your users, there may be a small delay in expanding/collapsing tree nodes. If this is the case, you can display a loading animation icon during the expand/collapse process - so your users are aware something is in progress. This generally isn't required, but may be desirable if you have 500+ Password Lists/ Folders.

## When generating a password based on a Password Generator Policy, perform the following number of retries to ensure the password

© 2014 Click Studios (SA) Pty Ltd

## meets the strength of the selected Password Strength Policy

When using the Password Generator feature to generate new passwords for a Password List, the Password Generator tries to create a password which matches the Password Strength Compliance level set for the Password List. Depending on the settings for the selected Password Generator Policy, it's possible the generating of passwords may get itself in an endless loop trying to match the Password Strength Compliance level, so this setting tells the generator when to give up trying and simply use the last generated password.

## Limit the size of scheduled HTML email reports to

All the available reports on the 'Reports' screen can be sent as either csv attachments, or embedded HTML within the email. If your users choose embedded HTML, large reports can cause performance issues when trying to open and read the email. This option allows you to specify the maximum size of the report. If the maximum size is reached, the user is information of this within the email, and they are recommended to change the report to a csv attachment.

## Use regular expressions when matching 'Bad Passwords'

If the use of 'Bad Password' detection is enabled on the Password Options Tab, the use of regular expression matching means the bad password can be detected anywhere within the string, not just the bad password on it's own i.e. mypassword would be deemed as a bad password, as it contains the word password.

## Enable option for purging of Auditing records

If you don't want to give Security Administrators the ability to purge (delete) auditing records on the Auditing page, then you can hide the controls which allow the purging.

## When users are 'Requesting Access' to passwords, hide the following fields due to possible sensitive information being stored in them

From the 'Passwords' menu at the bottom of the screen, users are able to request access to either Password Lists or individual Passwords they don't already have access to - assuming you have enabled this feature for them. As viewing password related data can be sensitive by its very nature, you can choose to hide various fields on the screen from your users, either the Username, Description or Notes fields.

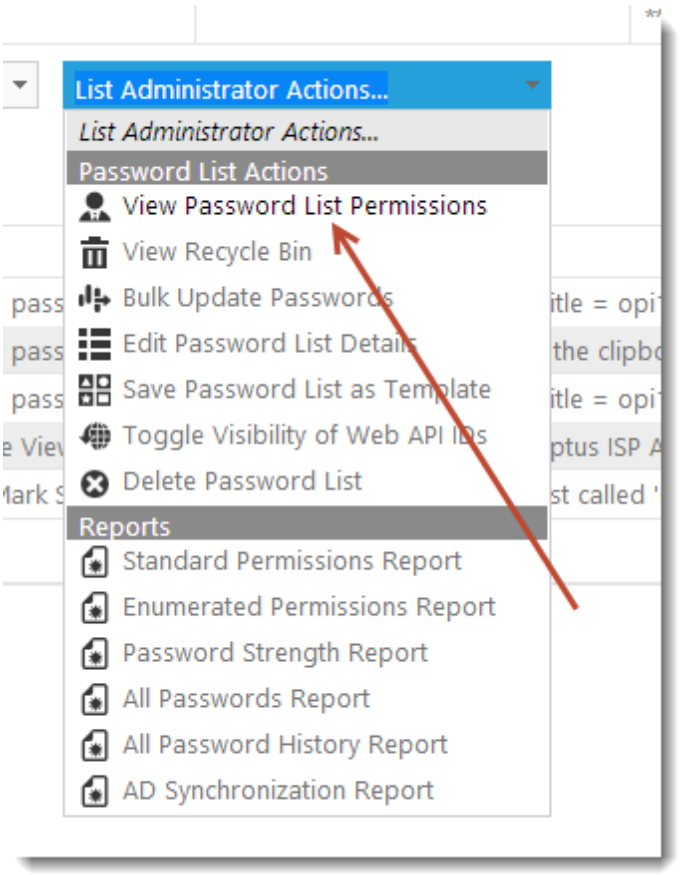
## Allow permissions to be applied multiple times for a user/security group to the same Password or Password List

Under certain circumstances, you may wish to allow the application of multiple permissions to a Password List or Password record for user accounts or security groups. If this is a requirement, you can check this option.

© 2014 Click Studios (SA) Pty Ltd

## Allow users to view Password List permissions when they are not Administrators of the Password List

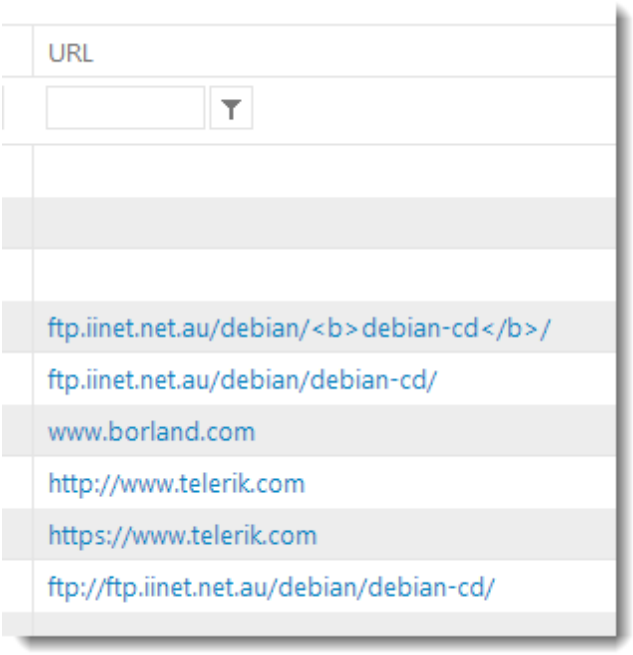
Under each Password List grid there is a drop-down list called 'List Administrator Actions'. The majority of options in this drop-down list are only accessible to Administrators of the Password List. If a user does not have Administrators rights to the Password List, it might still be useful if they can see what other users or security groups have access to the Password List. By enabling this option, the 'View Password List Permissions' feature will be available to them - they will only be able to view permissions, not change them.



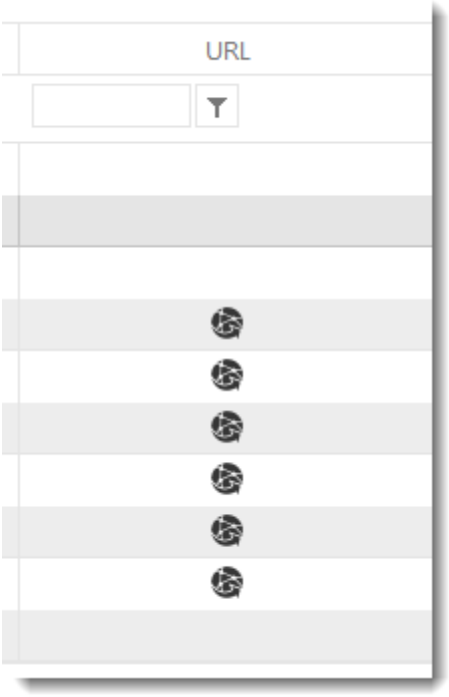

**When displaying URL columns in grids, display the URL value as a**

If you have chosen the URL field for any one of the Password Lists, there are two formats the URL can be displayed in when viewed in the Passwords grid - either a hyperlink text field, or hyperlink Icon - both of which will launch the URL when clicked on. They are displayed in the following manner:

© 2014 Click Studios (SA) Pty Ltd




Or




## 23.2 Password List Options Tab

The Password List Options Tab provides multiple settings which are applicable to Password Lists in Passwordstate.

© 2014 Click Studios (SA) Pty Ltd

## Allow users to export details from their private Password Lists

If you wish to prevent users from exporting passwords from their Private Password Lists, you can do so by selecting this option.

## Select which Code Page to use when Importing or Exporting data

When importing or exporting data, you can specify the default Code Page which will be used for character encoding - A Code Page consists of a table of values that describes the character set for a particular language. By default, all Password Lists will use the Code Page you specify here, but can be changed to use a different Code Page by editing the Password Lists settings.

## Modify permissions for Password Lists can

When a user is given 'Modify' permissions to a Password List, the default options allows the user to add new passwords, and edit or delete existing passwords. You can modify this default behavior by unchecking one or more options here.

## Enable the Automatic Password Rotation option for

The Automatic Password Rotation feature allows you to automatically generate a new password when the current one 'expires' and then synchronize this password with the Active Directory or Local Windows Server account. Depending on your requirements, you may disable this feature for both Shared and Private Password Lists if required.

## When creating new Shared Password Lists, base the settings on the following Template's settings

When your users create new Password Lists, you can specify a template here as a basis for the new Password List's settings. This allows you to provide some consistency across multiple Password Lists if required.

Note: This setting does not affect Private Password Lists.

## When creating new Shared Password Lists, base the permissions on the following Template's permissions

When your users create new Password Lists, you can specify the initial permissions should be copied from the selected Template. If required, there's also an option below to add permissions for the creator of the Password List as well.

Note: This setting does not affect Private Password Lists.

## Allow users to override the Template based settings above for new Shared Password Lists, with a Template they select in their

© 2014 Click Studios (SA) Pty Ltd

## 'Preferences' area

In addition to setting a Template above as the default settings for newly created Shared Password Lists, users can by default specify their own template to use in the 'Preferences' area. If you wish to enforce a single Template to be used by all users, you can do so with this option.

## When creating new or editing existing Shared Password Lists, if the user copies settings from a Template, then select the 'Link To Template' option by default

When you add a new Shared Password List, or edit the settings for an existing one, there is an option to copy settings from a selected Template, and also link the Password List to the Template. This option allows you to specify whether the check-box for linking to the Template is checked or unchecked by default.

## When users create a Password List and copy permissions from another Password List or Template, also add permissions for the user creating the Password List

When creating new Shared Password Lists, if permissions are being copied from another Password List or Template, this option allows you to also add permissions for the user who is creating the Password List - so instead of just cloning permissions, you can clone plus add the 'creator's account as well.

## When copying settings from a Template to a Password List, also copy the following field values

By default, the Password List Name and Description fields aren't populated when copying settings from another Password List or Template. With these two options you can choose to copy them if needed.

## Allow users to create password records when they only have Guest permissions to the Password List

When a user is given access to individual passwords in a Password Lists, as opposed to permissions being applied to the Password List itself, the user is given 'Guest' rights to the entire Password List. This is so the Password List will show in the Navigation Tree on the left-hand side of the main screen. By selecting this option, you will allow users who have Guest access to also create new passwords in the selected Password List.

Note: If this option is enabled a user creates a new Password record, they will be given Modify rights to the individual Password record they are creating.

© 2014 Click Studios (SA) Pty Ltd

## Allow users to copy/move/link passwords to Password Lists which they have View access to

It's possible for your users to copy or move passwords around between different Password Lists they have access to. By selecting this option, you allows them to copy/move/link passwords into Password Lists they only have View Access to. If deselected, they will only be able to do so to Password Lists they have Modify or Admin access to.

## When copying/moving/linking passwords between Password Lists, allow users to view all Password Lists, not just the ones they have access to

When your users copy/move/link passwords between different Password Lists, by default they will only be able to see the 'destination' Password Lists on the screen which they have been given access to. It's possible you may have a requirement to allow them to copy/move/link into Password Lists they don't have access to, and by selecting this option they will be allowed to do this.

## When searching for users in order to grant them access to Password Lists, only show users who are in the same Security Groups as the person granting the access

In the main 'user' screens of Passwordstate (i.e. not the Administration area), there are various screens where you can apply permissions for users accounts. By selecting this option, they will only be able to see/search for users who are in the same Local or Active Directory Security Groups as themselves - as they are recorded in Passwordstate.

## When a new Password List is created, apply the following permission to the user who created the list

When new Password Lists are created, the default option is to provide the user Administrative rights to the Password List. If required, you can change this default behavior to either Modify or View permissions

## When new Shared Password Lists are created, grant Security Administrators with the selected role below admin rights to the Password List

As new Password Lists are created, you can also choose to automatically grant one or more Security Administrators of Passwordstate administrative rights to the Password Lists. You can do this by selecting the 'All Security Administrators' option, or just the ones who are assigned a specific Security Administrator role.

© 2014 Click Studios (SA) Pty Ltd

## 23.3 Password Options Tab

The Password Options Tab has multiple settings applicable to Password values being visible on the screen, clearing the clipboard, and Bad Password detection.

### Synchronize the 'Deleted' status of Linked Password records across all affected Password Lists

When Password records are copied & linked between different Password Lists, you can use this option to specify whether all of the 'linked' records are moved to the Recycle Bin when one of them is deleted. If the option is not selected, the other linked records will remain visible in each of their respective Password Lists.

### When users add/edit passwords, alert them when a 'Bad Password' is specified and rate it as

When your users add or edit password records, you can choose to either alert them when 'bad passwords' are detected, as per the list stored in the Bad Passwords screen, or you can allow bad passwords to be used. If a bad password is detected, you can specify why Password Strength indicator you would like to be assigned to the password record.

### Automatically clear clipboard after the following specified number of seconds

When your users copy Passwords to the clipboard using the icon, you can specify how long before the clipboard is automatically cleared.

Note: This option is only applicable to Internet Explorer, as it's not possible to automatically clear the clipboard with Firefox or Chrome - a button will appear at the top right-hand side of the screen allowing you to clear the clipboard if required.

### When Password masking is displayed on the grid views (*****) show a fixed character length of

It's possible to use 'Fixed Length Password Masking' in Passwordstate, as an added security measure. By using this feature, the screens which show a masked password like ****** will all be of the same length, regardless of how many characters the Password field consists of.

### Automatically hide visible passwords based on the following conditions (in seconds)

By clicking on any masked passwords in the grid view, i.e. *******, or the icon on any of the add/edit/view password screens, the password will be revealed to you. There are 3 different options for how quickly you wish to password to again be masked, and they are:

© 2014 Click Studios (SA) Pty Ltd

- Set Time - one set time period for all passwords, regardless of their length and complexity
- Password Complexity - here you can specify 5 different time intervals, each for the different Password Strength ratings
- Password Length - here you can specify up to three different time periods based on the length of the password fields i.e. if the password field is 20 characters in length, you probably would need it to be displayed longer on the screen compare to a record which is only 5 characters long

## 23.4 Email Alerts & Options Tab

The Email Alerts & Options Tab allows you to specify your email servers settings, so emails can be generated from Passwordstate, as well as multiple settings and notifications relating to emails being sent.

### Send email alerts to Security Administrators (who have User Accounts role) for Failed Login Attempts

There are two different scenarios in which your users must authenticate when using Passwordstate:

1. When they first browse to the web site
2. If a Password List is configured to require an 'Additional Authenticate' step prior to the Password List being accessible

By selecting this option, Security Administrators who have the 'User Accounts' role will be alerted, via email, to any failed login attempts. Failed login attempts are also recorded and reportable on the Auditing screens.

### Only send Failed Login Attempt email alerts to Security Administrators if the following conditions are met

If Security Administrators don't wish to be alerted to every single failed login attempt by individual users, you can set a threshold which must be met before an email is sent. Even if this option is used to not be notified every single time, auditing data is recorded for all failed login attempts.

### Alert Security Administrators if there are an excessive number of events (from a single user) for Viewing, Copying or Exporting Passwords. Alert if the following condition is met

Another option which alerts to uncommon behavior is to notify Security Administrators when an individual user is viewing, copying or exporting a lot of password data within a set period of time i.e. if a user views 10 password records within a single minute, then this is not common behavior and you may have an issue with potential information leakage/theft.

© 2014 Click Studios (SA) Pty Ltd

## When users 'Request Access' to Passwords or Password Lists, in addition to emailing the request to Password List Administrators, also email it to Security Administrators with the following roles

By default, Password or Password List Access Requests are routed to the Administrators of the relevant Password Lists. If you would also like the access requests to be sent to various Security Administrators, you can use this option to choose which Security Administrator roles will receive the requests

## When users 'Request Access' to Passwords or Password Lists, if there are no Administrators assigned to the Password List, email the request to Security Administrators with the following roles

It's possible that there may be no 'Administrator' permissions assigned to a Password List for your users - only Modify or View permissions. If this is the case, someone needs to be notified when users request access to passwords in a Password List which is configured this way. You can use this option to specify where the request is routed i.e. which Security Administrators will receive the 'Request Access' email and popup notification.

## Send email alerts to Security Administrators (with the following role) when passwords are exported

If you would like to alert your Security Administrators when users are exporting password data, you can use this option to do so.

## Send email alerts to Security Administrators (with the following role) if tampering of the Auditing table is detected

It's possible, but unlikely, that one of your users may try to edit/delete auditing data directly in the database, in attempt to conceal behavior they don't wish to be reported. By using this option, you can alert Security Administrators of any such activity. In the event tampering is detected, Security Administrators will be able to view which records have been affected, and also compare what data has been modified, facilitating an investigation if required.

## Use the following settings to send emails from within Passwordstate

As various functions are performed in Passwordstate, email records will be generated and stored in the QueuedEmail table. The Passwordstate Windows Service checks this table once every minute, and sends the emails if any exist. In order for emails to be sent, you need to specify various settings for your email server. In particular:

- Host Name and Port Number
- Which SMTP address you would like the emails to be sent from
- Whether or not your email server is configured to send via TLS (Transport Layer Security)

© 2014 Click Studios (SA) Pty Ltd

- And if you need to specify an account to send from i.e. Sending Anonymous SMTP emails is not allowed from your email server

Note: If the account stored for this setting is also stored in a Password List which is enabled for synchronizing of passwords into Active Directory or local Windows Servers, then this password below will also be updated when a synchronization occurs.

## 23.5 Proxy & Syslog Servers Tab

The Proxy & Syslog Servers Tab allows you to specify proxy server details to allow querying the Click Studios web site for new builds or Passwordstate, or Syslog server details to send all auditing data to.

### Proxy Server Details

To check for new builds of Passwordstate, you may need to specify your internal proxy server details, and possibly an account which can authenticate with your proxy server if required.

Note 1: If the account stored for this setting is also stored in a Password List which is enabled for synchronizing of passwords into Active Directory or local Windows Servers, then this password below will also be updated when a synchronization occurs.
Note 2: If you are concerned about your Passwordstate web site accessing the Internet, the only file we access is http://www.clickstudios.com.au/NewBuildInfo.xml. No data can be sent or captured by reading an XML file, and you can run a program such as WireShark on your web server to confirm this is the only file Click Studio's checks

### Syslog Server Details

If required, you can send all Auditing data to one of your own internal SysLog servers. It is the Passwordstate Windows Service which checks every minute for new data to send, and the Windows Service keeps track of the latest auditing record which was successfully sent, and only send subsequent records.

## 23.6 Active Directory Options Tab

The Active Directory Options tab allows you to specify an account to interact with Active Directory, and various options for User Account, Security Group and Password synchronization.

### Active Directory Privileged Account Credentials

In order for Passwordstate to synchronize User Account enabled/disabled status in AD, Security Group Memberships, and passwords between Passwordstate and Active Directory/Windows Servers, you must specify a domain account to use with sufficient privileges to perform these tasks.

© 2014 Click Studios (SA) Pty Ltd

Note 1: If the account stored for this setting is also stored in a Password List which is enabled for synchronizing of passwords into Active Directory or local Windows Servers, then this password below will also be updated when a synchronization occurs.
Note 2: If you don't plan on using Passwordstate to synchronize Passwords with Active Directory or Windows Servers, then the account you specify here only needs permissions to read from Active Directory
Note 3: You can also specify which users in Passwordstate are allowed to synchronize passwords with Active Directory and Windows Servers via the Password Synchronization Options tab

## Passwordstate User Account and Security Group Membership Options

The 'Passwordstate User Account and Security Group Membership Options' settings allows you to specify various options for synchronizing User Account enabled/disable status, and security group memberships within Passwordstate.

**If a User Account is found within a Security Group which hasn't already been added to Passwordstate, would you like to automatically add the User Account;**
When the Passwordstate Windows Service synchronizes the membership of any Security Groups you've added on the Security Groups screen, it's possible there will be user accounts in the Active Directory security group which have not yet been added to the User Accounts screen. If this is the case, you can use this option to automatically add the accounts to Passwordstate, or simply ignore the account.

Note: If you reach the maximum number of Client Access License as recorded on the License Information screen, the user accounts will not be added to Passwordstate.

**Synchronize the enabled/disabled status of Active Directory user accounts with the user accounts in Passwordstate;**
Using this option, if the enabled/disabled status of a user account in Active Directory is changed, you can also synchronize that change to the account stored in Passwordstate.

**When an account in Active Directory is deleted, perform the following in Passwordstate:**
If a User Account in Active Directory is deleted, you can choose either you want to delete it in Passwordstate, disabled the account, or simply do nothing.

**When a user is removed from a Security Group, and that user no longer belongs to any Security Groups, perform the following in Passwordstate:**
If a user no longer belongs to any Active Directory Security Groups, which have been added to Passwordstate, you can choose to delete, or do nothing with their account

Note: For the two options above, if you choose to delete the user account in Passwordstate, all access for the user's account will be removed, and any Private Password Lists they may have had will be deleted.

**Synchronize Security Group Memberships, and User Account status at:**

© 2014 Click Studios (SA) Pty Ltd

Synchronizing of Active Directory security group memberships, and the status of user accounts (either enabled, disabled or deleted status), can be done either once a day or more frequently if required, by choosing the appropriate option here.

Performance Tip: If you have many Active Directory User Accounts added to Passwordstate, the synchronization of the features above will perform significantly better if these user accounts belong to one or more Security Groups, and these Security Groups have also been added to Passwordstate via the page Security Groups. The reason for this performance improvement is because all the users can be enumerated with one call to Active Directory for the Security Group, instead of making separate calls for every single account. If you have many AD users added to Passwordstate (i.e. 200+), it is recommended you add one or more Security Groups even if you don't use them to apply permissions anywhere.

## 23.7 Authentication Options Tab

The Authentication Options Tab provides various settings for when your users first authenticate to the Passwordstate web site.

Note 1: Options will be different on this screen, depending on if you have installed the Active Directory integrated version of Passwordstate, or the Forms-Based Authentication version.
Note 2: If in the event you lock yourself out of authenticating against the Passwordstate web site for any reason, you can always use the Emergency Access account to authenticate.

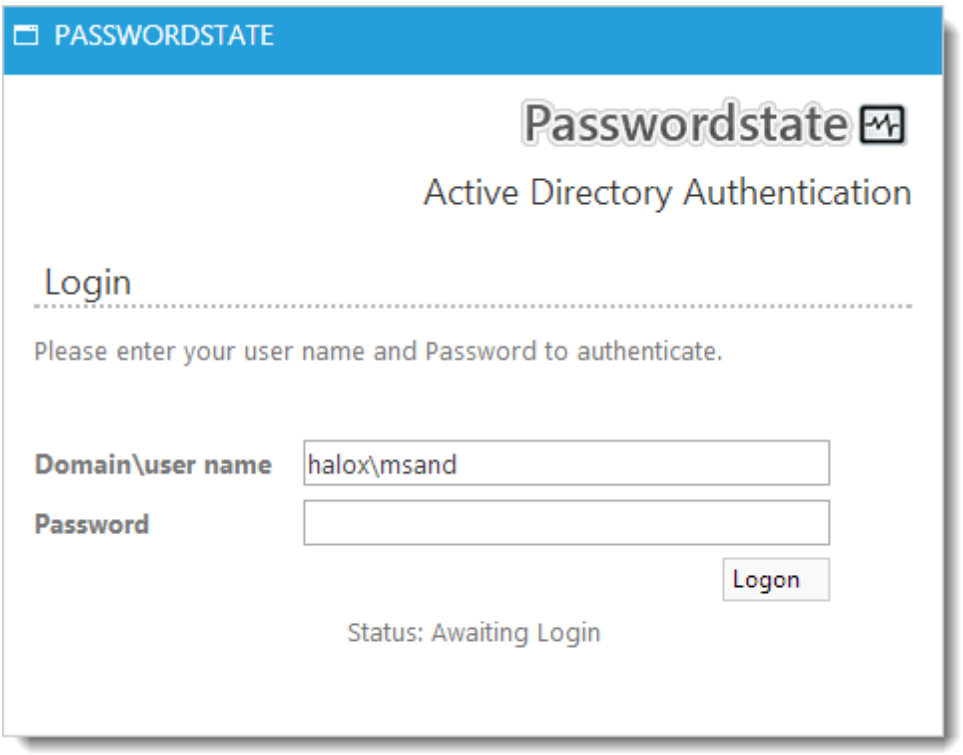
### Authentication Option

There are multiple different authentication options available for when your users first access the Passwordstate web site, and they are:

**Passthrough AD Authentication**
If DNS, your browser, and the site in IIS is configured correctly, your browser should not prompt you for your account details when using this authentication method, instead it should pass your account details to the Passwordstate web site in IIS, and IIS ensures your account exists in Active Directory.

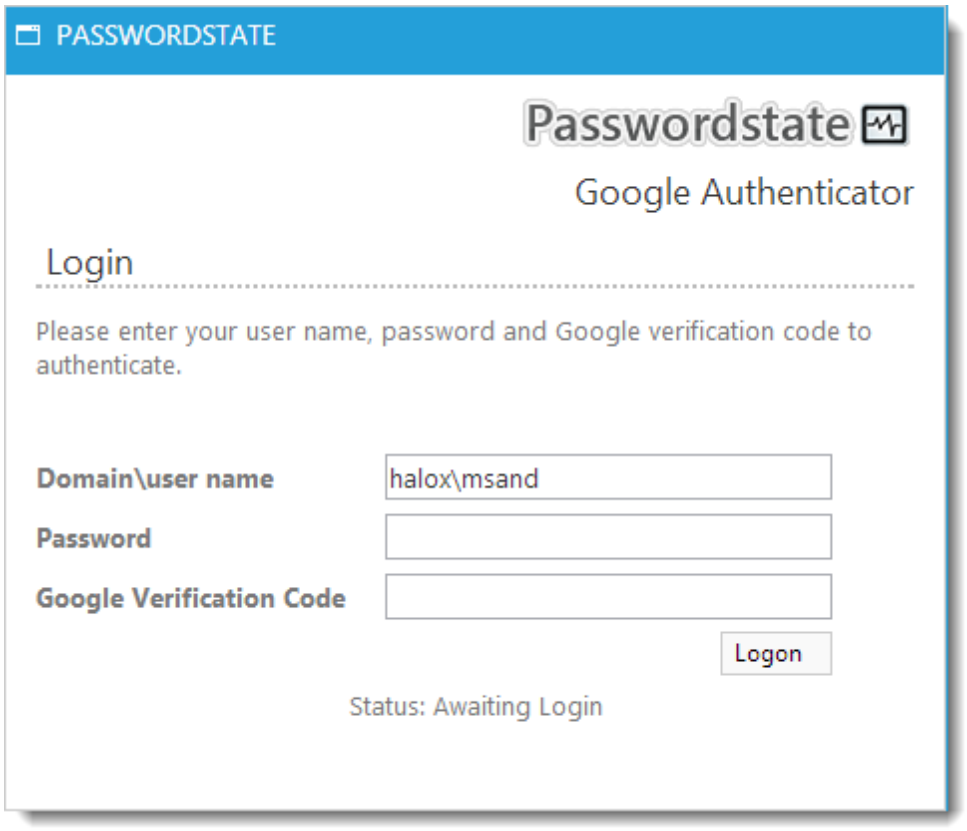
**Manual AD Authentication**
Provides a dialog for users to manually specify their AD domain credentials.

© 2014 Click Studios (SA) Pty Ltd




**Manual AD and Google Authenticator**
Provides a dialog for users to manually specify their AD domain credentials, and a Google Verification Code. To use this authentication method, the user must create a Google Authenticator Secret Key on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

© 2014 Click Studios (SA) Pty Ltd



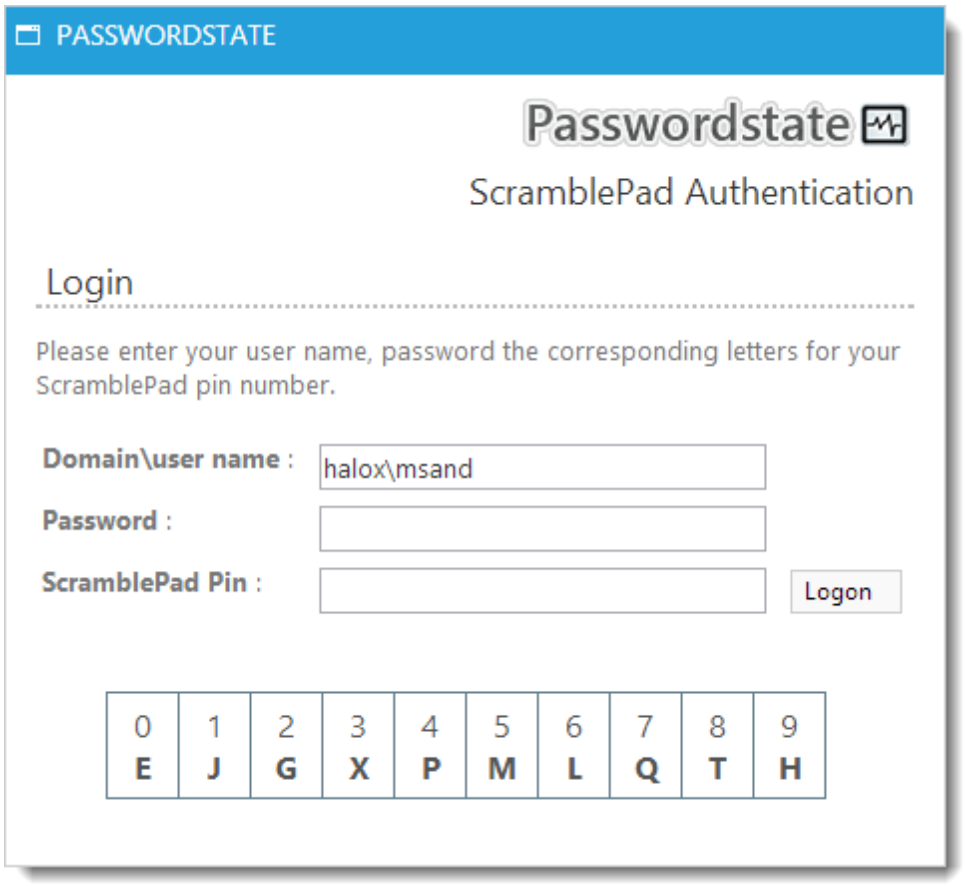

**Manual AD and RSA SecurID Authentication**
Provides a dialog for users to manually specify their AD domain credentials, and a SecurID Passcode. To use this authentication method, the user must have a valid SecurID account and token.

© 2014 Click Studios (SA) Pty Ltd

**Manual AD and ScramblePad Authentication**
Provides a dialog for users to manually specify their AD domain credentials, and a ScramblePad Pin. To use this authentication method, the user must specify their ScramblePad Pin number on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

In the screenshot below, if the user's Pin Number was **0123**, then they would need to enter **ejgx** to authenticate correctly - the letters are rearranged every time the screen is accessed.

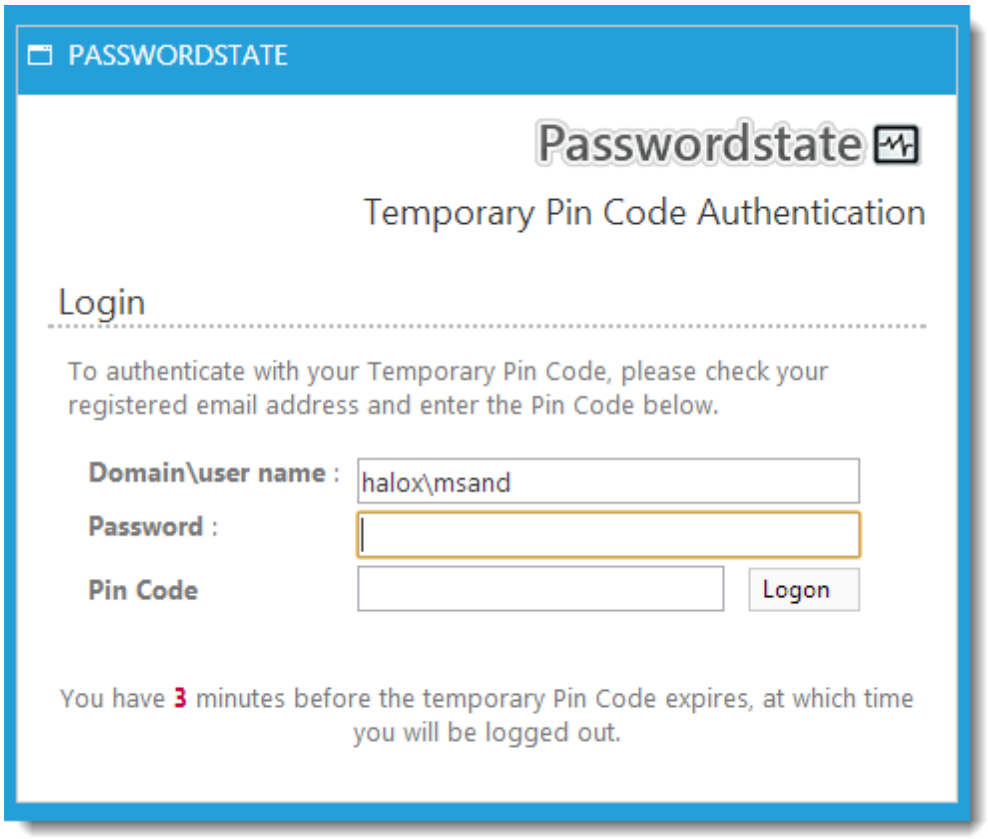
© 2014 Click Studios (SA) Pty Ltd




**Manual AD and Email Temporary Pin Code**
Provides an authentication dialog for users to manually specify their own AD credentials, and also a Temporary Pin Code. User's must specify an email address in their 'Preferences' area as to where they want the Temporary Pin Code to be emailed to, and Security Administrators cannot set this email address for them.

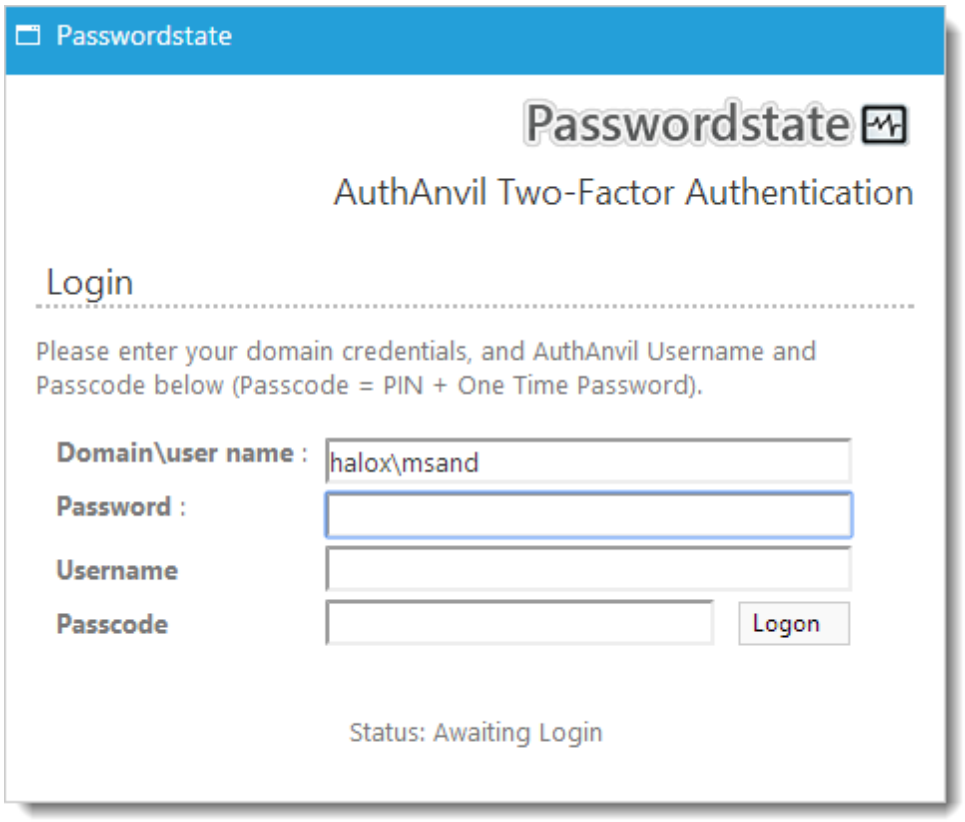
The length of the Pin Code, and the time in which it expires, can also be set on this screen.

© 2014 Click Studios (SA) Pty Ltd


PASSWORDSTATE
Passwordstate
Temporary Pin Code Authentication
Login
To authenticate with your Temporary Pin Code, please check your registered email address and enter the Pin Code below.
Domain\user name :
halox\msand
Password :
Pin Code
Logon
You have 3 minutes before the temporary Pin Code expires, at which time you will be logged out.

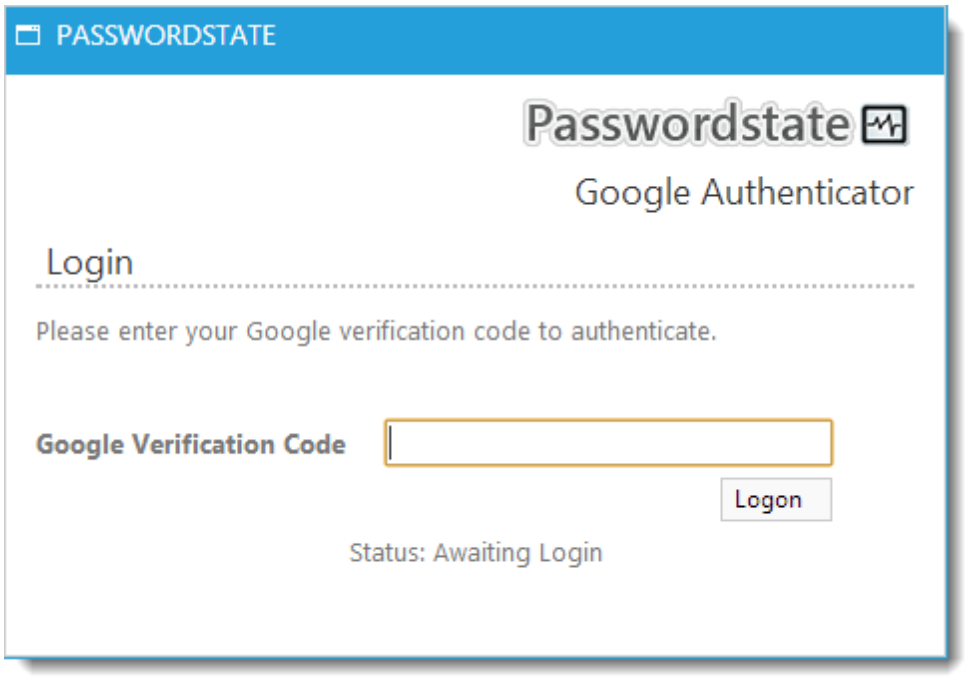
**Manual AD and AuthAnvil Authentication**
Provides a dialog where you can enter both your Active Directory domain credentials, and your AuthAnvil Username and Passcode to log in using two-factor authentication. User's must have specified their AuthAnvil Username on the Preferences screen in order to authenticate.

© 2014 Click Studios (SA) Pty Ltd

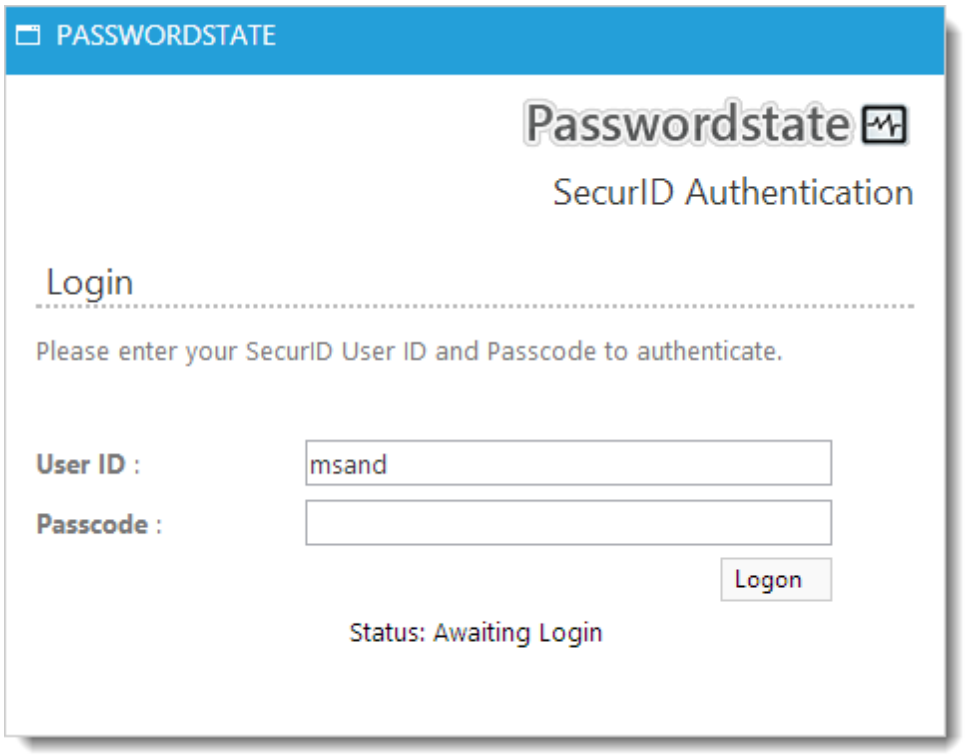



**Google Authenticator**
Provides a dialog for users to manually specify their Google Verification Code - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must create a Google Authenticator Secret Key on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

© 2014 Click Studios (SA) Pty Ltd



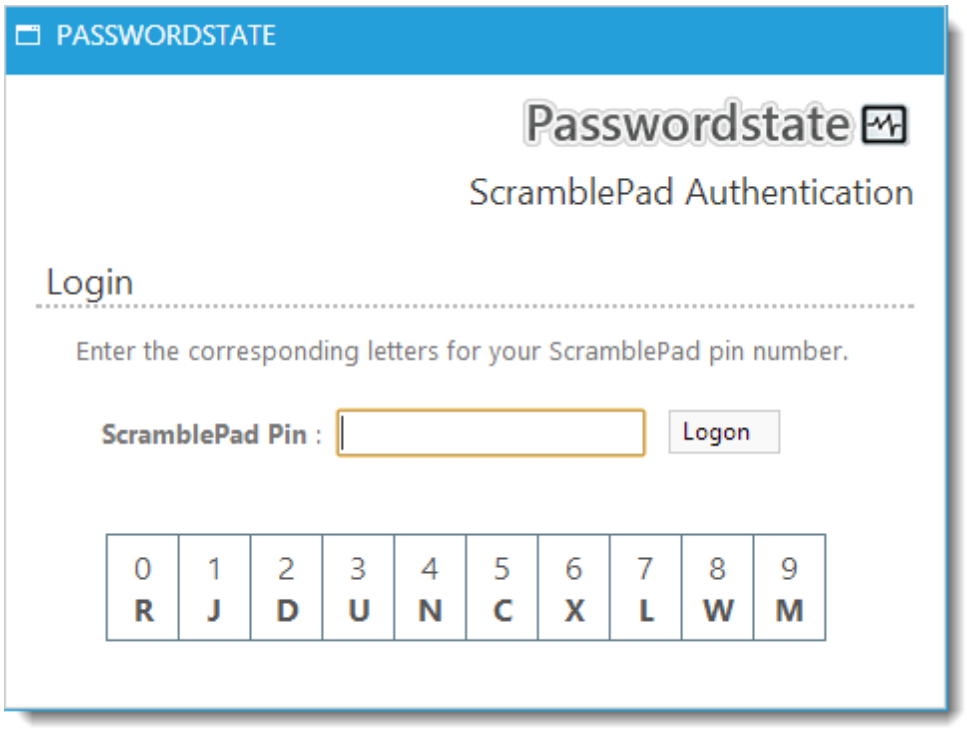

**RSA SecurID Authentication**
Provides a dialog for users to manually specify their SecurID Passcode - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must have a valid SecurID account and token.




© 2014 Click Studios (SA) Pty Ltd

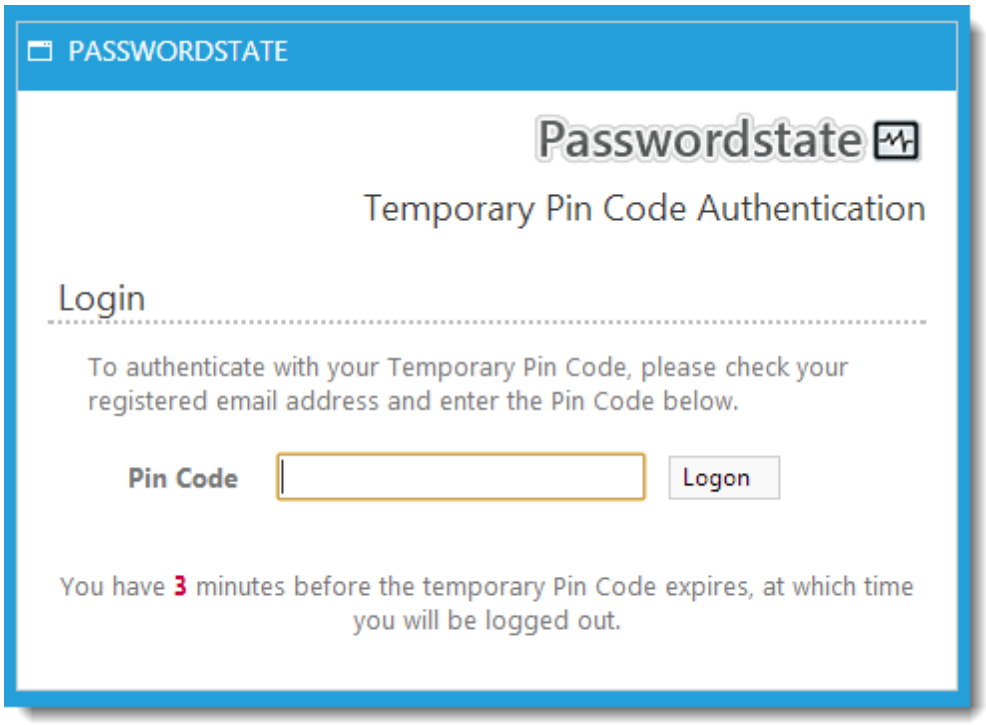
**ScramblePad Authentication**
Provides a dialog for users to manually specify their ScramblePad Pin code - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must specify their ScramblePad Pin number on the Preferences screen, or Security Administrators can do it for them on the User Accounts screen.

In the screenshot below, if the user's Pin Number was **0123**, then they would need to enter **rjdu** to authenticate correctly - the letters are rearranged every time the screen is accessed.

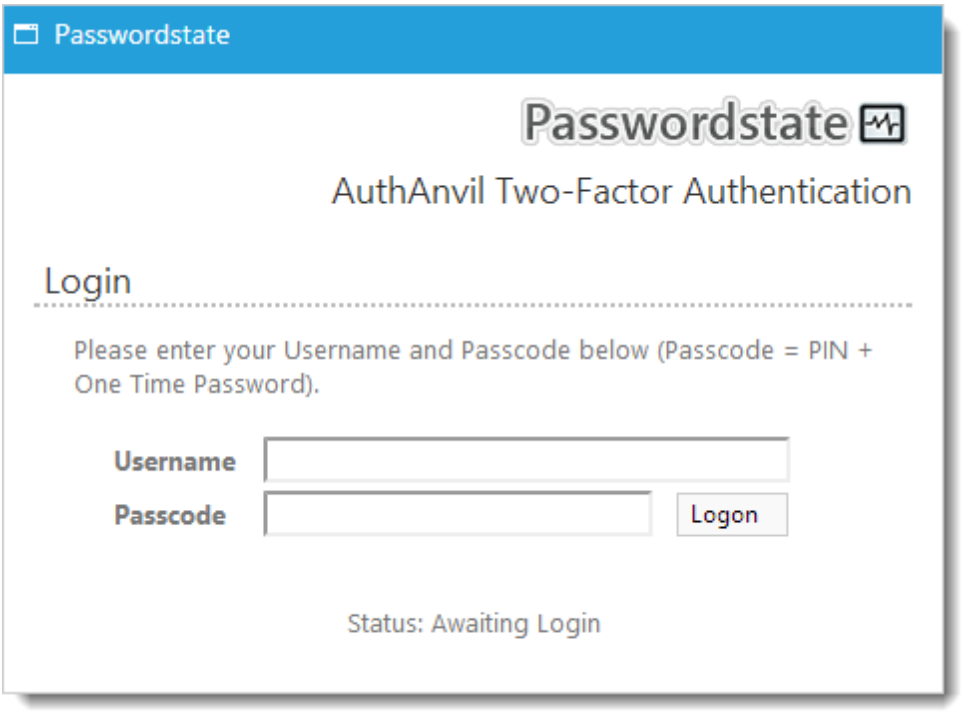



**Email Temporary Pin Code**
Provides an authentication dialog for users to enter a Temporary Pin Code. User's must specify an email address in their 'Preferences' area as to where they want the Temporary Pin Code to be emailed to, and Security Administrators cannot set this email address for them.

© 2014 Click Studios (SA) Pty Ltd

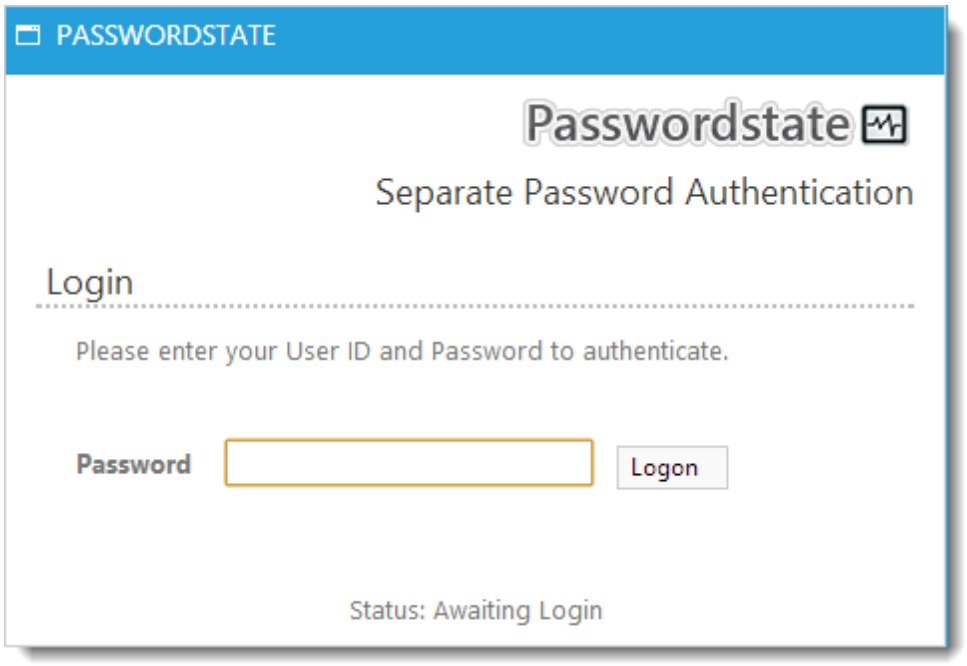

PASSWORDSTATE
Passwordstate
Temporary Pin Code Authentication
Login
To authenticate with your Temporary Pin Code, please check your registered email address and enter the Pin Code below.
Pin Code
Logon
You have 3 minutes before the temporary Pin Code expires, at which time you will be logged out.

**AuthAnvil Authentication**
Provides a dialog where you can enter your AuthAnvil Username and Passcode to log in using two-factor authentication. User's must have specified their AuthAnvil Username on the Preferences screen in order to authenticate.




© 2014 Click Studios (SA) Pty Ltd

**Separate Password**
Provides a dialog for users to specify a separate authentication password - this works in conjuction with Passthrough AD Authentication. To use this authentication method, the user must specify their separate password on the Preferences screen, or Security Administrators can create a random password for them on the User Accounts screen.




## Various Authentication Options

Some of the authentication methods above also have various options which can be set, and they are:

**If one of the Manual AD Authentication options are selected, auto-populate the UserID field based on the current logged in Active Directory account**
If you select one of the 'Manual AD' authentication options for your users, you can automatically populate the UserID field for them if required.

**Auto-populate the SecurID UserID field for the user**
If you select one of the 'SecurID' authentication options for your users, you can automatically populate the UserID field for them if required.

**Make the SecurID UserID field on the login screen read only**
This option prevents a user from walking up to another user's computer, authenticating with their own SecurID Token, but then logging into Passwordstate as the other user - this can happen when the Passthrough authentication occurs after the SecurID authentication happens, as there does not necessarily need to be a correlation between a users SecurID user account and their domain account.

© 2014 Click Studios (SA) Pty Ltd

**When using the Forms-Based Authentication version of Passwordstate and a SecurID authentication option above, show just the SecurID authentication screen on initial login**
When this option is selected, you will not be prompted to enter your forms based UserID and Password, only your SecurID UserID and Passcode.

**Specify your AuthAnvil Web Services URL and SiteID here**
You must specify your AuthAnvil's Web Services URL and SiteID in order to use this two-factor authentication option. The URL is generally in the format of https://yourFullyQualifiedDomain.com/AuthAnvil/sas.asmx

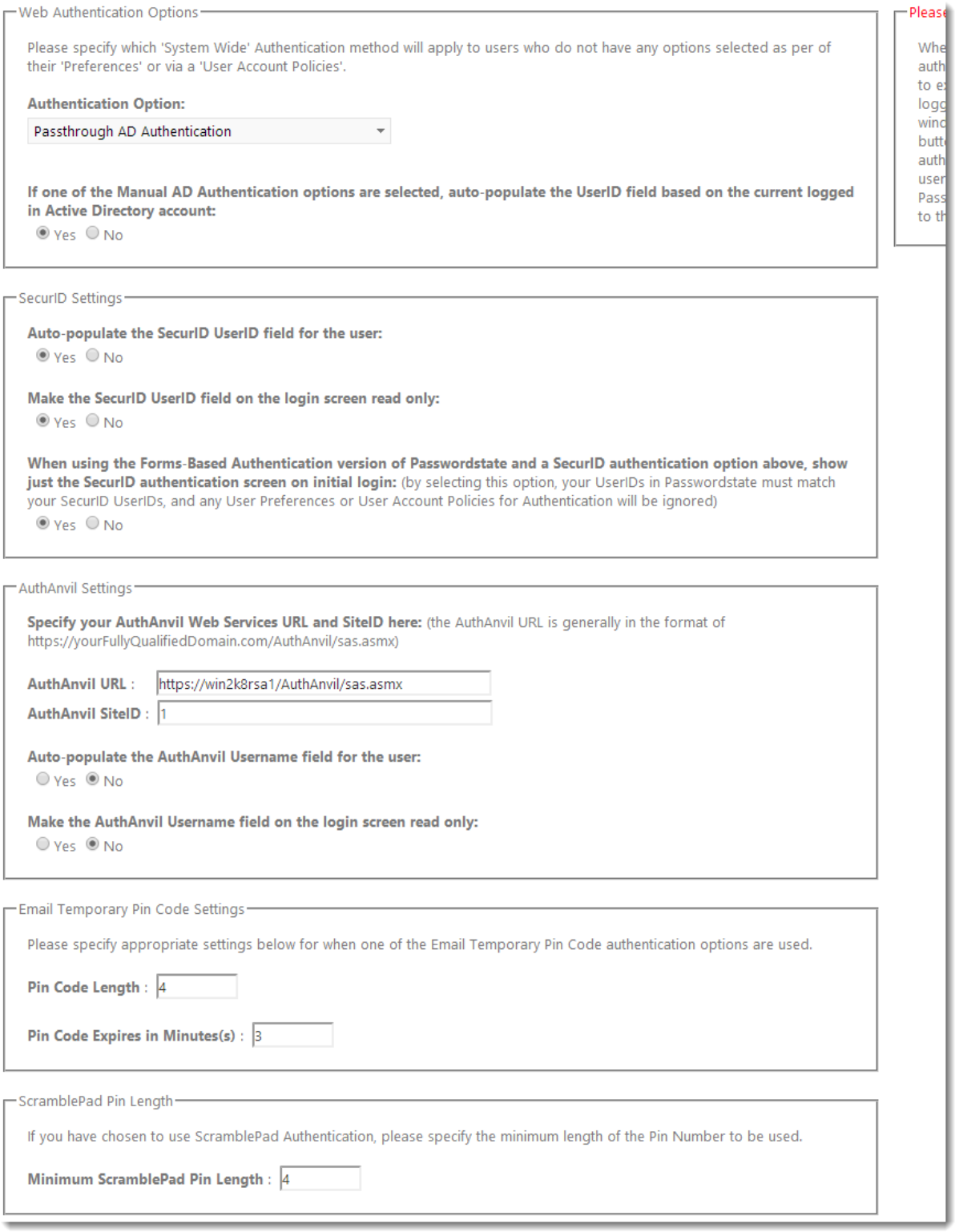
**Auto-populate the AuthAnvil Username field for the user**
If you select one of the 'AuthAnvil' authentication options for your users, you can automatically populate the Username field for them if required.

**Make the AuthAnvil Username field on the login screen read only**
This option prevents a user from walking up to another user's computer, authenticating with their own AuthAnvil Username and Passcode, but then logging into Passwordstate as the other user - this can happen when the Passthrough authentication occurs after the AuthAnvil authentication happens

**Email Temporary Pin Code Settings**
The Temporary Pin Code Settings allows you to specify the length of the Pin Code, and also how long until the temporary Pin Code will expire if not used.

**Minimum ScramblePad Pin Length**
By default, the ScramblePad Pin length is 4 characters, but can be changed if required.

© 2014 Click Studios (SA) Pty Ltd


Web Authentication Options
Please specify which 'System Wide' Authentication method will apply to users who do not have any options selected as per of their 'Preferences' or via a 'User Account Policies'.
Authentication Option:
Passthrough AD Authentication
If one of the Manual AD Authentication options are selected, auto-populate the UserID field based on the current logged in Active Directory account:
Yes No
SecurID Settings
Auto-populate the SecurID UserID field for the user:
Yes No
Make the SecurID UserID field on the login screen read only:
Yes No
When using the Forms-Based Authentication version of Passwordstate and a SecurID authentication option above, show just the SecurID authentication screen on initial login: (by selecting this option, your UserIDs in Passwordstate must match your SecurID UserIDs, and any User Preferences or User Account Policies for Authentication will be ignored)
Yes No
AuthAnvil Settings
Specify your AuthAnvil Web Services URL and SiteID here: (the AuthAnvil URL is generally in the format of https://yourFullyQualifiedDomain.com/AuthAnvil/sas.asmx)
AuthAnvil URL : https://win2k8rsa1/AuthAnvil/sas.asmx
AuthAnvil SiteID : 1
Auto-populate the AuthAnvil Username field for the user:
Yes No
Make the AuthAnvil Username field on the login screen read only:
Yes No
Email Temporary Pin Code Settings
Please specify appropriate settings below for when one of the Email Temporary Pin Code authentication options are used.
Pin Code Length : 4
Pin Code Expires in Minutes(s) : 3
ScramblePad Pin Length
If you have chosen to use ScramblePad Authentication, please specify the minimum length of the Pin Number to be used.
Minimum ScramblePad Pin Length : 4

© 2014 Click Studios (SA) Pty Ltd

# 23.8 Password Synchronization Options

Passwordstate can synchronize password changes with Active Directory, or the local accounts database on Windows Servers. This tab allows you to specify various settings and permissions for this feature.

## Active Directory and Windows Server Accounts

In Passwordstate you can configure a Password List to synchronize the password records with Active Directory if required. This could be user accounts on the domain, or accounts you have created to act as "service accounts".

For detailed instructions of how to configure permissions and use the Password Synchronization feature in Passwordstate, please see the Knowledge Base article '**Synchronize Passwords with Active Directory on Windows Servers**' in the User Manual.

Note 1: You can only synchronize passwords from Passwordstate into Active Directory, not the other way around - it's not possible to decrypt the values of AD passwords.
Note 2: If you change the domain account used here, or modify the permissions for this account i.e. add to a new security group, then it is recommended you restart the Passwordstate Windows Service.

**When synchronizing passwords with Active Directory or Windows Server, validates the passwords match before allowing a password to be changed:**
If this option is set to Yes, then it will first check if the password stored in Passwordstate matches what's stored in AD/Windows Server, prior to performing any new synchronizations. This can act as a security measure to prevent users of Passwordstate making changes to AD/Windows Server accounts if they don't know what the password currently is i.e. prevents them from adding a record with any password value, and then performing a synchronization

**Enable the Password List setting of 'Show Active Directory & Windows Actions for Passwords which are enabled for Sync':**
If this option is enabled, then it can be selecting a part of the settings for a Password List. When selected, it will provide a new Tab on the Edit Password screen which allows you to do the following to the account in Active Directory/Windows Server:

- Unlock the account if locked
- Set the option 'User must change password at next logon'
- Disable the account
- Enable the account

## Enable Synchronization With Permissions

Each Shared Password List or Template can be configured to synchronize passwords with either Active Directory, or the local accounts database on Windows Servers. You may not want all users

© 2014 Click Studios (SA) Pty Ltd

be able to configure these settings, so by clicking on the 'Set Permissions' button you can specify what User Accounts or Security Groups are allowed to configure settings for this feature.

## 23.9 Mobile Access Options

The Mobile Access Options tab allows you to specify multiple settings for how the Passwordstate Mobile Client behaves for your users.

### Allow Mobile clients to access Passwordstate:

If you do not wish to allow Mobile Access to passwords, you can disable access altogether by selecting this option.

Note 1: If you choose to disable Mobile Access, it is recommended you set the option below to 'No', and then go to the screen Administration -> Passwords Lists -> Mobile Access Bulk Permissions, and then disable Mobile Access for all permissions
Note 2: Even if this option is enabled, your Firewall/System Administrators still need to configure external DNS and allow access through the firewall for anyone to access the Mobile Client web site

### When adding new permissions to Password Lists, enabled Mobile Access by default:

When adding new permissions to a Password List, you can use to enable/disable Mobile Access by selecting the appropriate option here.

### Use the following authentication method for the Mobile Client:

There are four types of Authentication Options available for the Mobile Client:

- Mobile Pin Number - a numeric pin code that the user can specify on their Preferences screen
- Active Directory Authentication - authenticate using the users Active Directory UserID and Password
- Email Temporary Pin Code - Two-Factor Authentication using the emailing of a temporary pin code, which expires after a set period of time
- AuthAnvil Authentication - Two-Factor Authentication using Scorpion Software's AuthAnvil solution

### The Mobile Access Pin Number for user authentication must be a minimum length of:

You can choose the length of the Mobile Access Pin Number the users must use to authenticate with. When the users specify their own Pin Number on the Preferences screen, or use the option

© 2014 Click Studios (SA) Pty Ltd

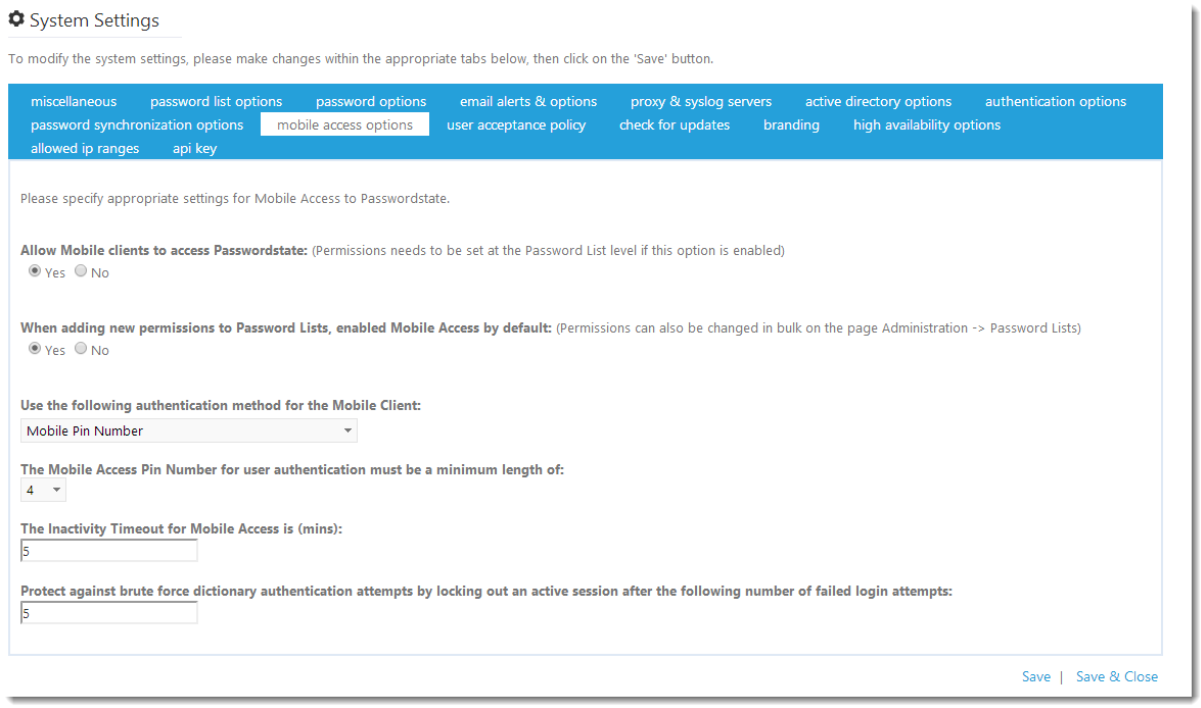
to generate one, it must meet the minimum length requirement of this setting.

## The Inactivity Timeout for Mobile Access is (mins)

If the user forgets to log out of the Mobile session, this setting will automatically log them out after the set period of inactivity, and also clear their authenticated session.

## Protect against brute force dictionary authentication attempts by locking out an active session after the following number of failed login attempts:

As the Mobile Access web site is generally externally accessible from your internal network, this setting will mitigate against any brute force authentication attempts by locking out authentication attempts when this setting has been reached.


System Settings
To modify the system settings, please make changes within the appropriate tabs below, then click on the 'Save' button.
miscellaneous
password list options
password options
email alerts & options
proxy & syslog servers
active directory options
authentication options
password synchronization options
mobile access options
user acceptance policy
check for updates
branding
high availability options
allowed ip ranges
api key
Please specify appropriate settings for Mobile Access to Passwordstate.
Allow Mobile clients to access Passwordstate: (Permissions needs to be set at the Password List level if this option is enabled)
Yes
No
When adding new permissions to Password Lists, enabled Mobile Access by default: (Permissions can also be changed in bulk on the page Administration -> Password Lists)
Yes
No
Use the following authentication method for the Mobile Client:
Mobile Pin Number
The Mobile Access Pin Number for user authentication must be a minimum length of:
4
The Inactivity Timeout for Mobile Access is (mins):
5
Protect against brute force dictionary authentication attempts by locking out an active session after the following number of failed login attempts:
5
Save | Save & Close

# 23.10 User Acceptance Policy Tab

The User Acceptance Policy Tab allows you to specify a popup 'User Acceptance Policy' (UAP) which users must read when they access the Passwordstate web site.

A default body of text is provided, but it can be customized to suite your organization.

© 2014 Click Studios (SA) Pty Ltd

There are also a couple of options for the UAP:

- No policy Required
- Yes - Mandatory for each new session (every time your users initiate a new session when they visit the site, they will be presented with the UAP popup)
- Yes - Acceptance Required (Once the user has read and accepted the policy, they will not be prompted again)

## 23.11 Check for Updates Tab

The Check for Updates Tab allows you to specify how frequently the Passwordstate web site should check for new updates, and who it should display the new build notification to.

This feature queries the following file - www.clickstudios.com.au/NewBuildInfo.xml, and if a new build is found, the notification will be displayed at the top left-hand side of the screen, just next to the main logo.

Note: Depending upon your environment, you may need to specify proxy authentication details on the Proxy & Syslog Servers Tab for this feature to work.

## 23.12 Branding Tab

The Branding Tab allows you to specify your own custom Logos to use at the top left-hand side of the page, and on various Dialog windows, as well as your own custom Page Titles.

If possible, it is recommended you make your logos of the following size, so that they appear symmetrically correct on the site:

- Title Logo - 192 pixels Wide x 28 pixels High
- Dialog Logo - 196 pixels Wide x 30 pixels High

Note 1: The logos are stored within the database, and restarting the Passwordstate Windows Service will recreate the logos on the file system if they are accidentally deleted for any reason.
Note 2: Adobe Photoshop template files are also provided, allowing for easier creation of your own logos if required.

## 23.13 High Availability Options Tab

If you have purchased the High Availability option for Passwordstate, the High Availability Options Tab allows you to specify the following settings:

- How frequently the High Availability instance should check for new or updated logos and custom images. If there are any new or updated images, they will be written to disk on the schedule provided
- When a user accesses the High Availability instance of Passwordstate, you can send email alerts to Security Administrators with the selected following role(s). This is useful as the High

© 2014 Click Studios (SA) Pty Ltd

Availability instance is read-only, which means no auditing data is added to the database. This gives you the opportunity to investigate why the user is accessing the High Availability instance, when they should be accessing the Primary instance.

## 23.14 Allowed IP Ranges Tab

The Allowed IP Ranges Tab allows you to specify a range of IP Addresses where clients are allowed to access the Passwordstate web site, or make calls to the Passwordstate API.

Specifying IP Ranges can be done in the following format:

- 192.168.1.* (all addresses in the range of 192.168.1.0 to 192.168.0.255)
- 192.168.*.* (all addresses in the range of 192.168.0.0 to 192.168.255.255)
- 192.*.*.* (all addresses in the range of 192.0.0.0 to 192.255.255.255)
- 192.168.1.1-192.168.2.50 (just the addresses in the range of 192.168.1.1 to 192.168.2.50)
- 192.168.1.50 (just a single IP Address)

Note 1: Regardless of the settings you specify here, you will always be able to access Passwordstate if logged into your web server directly, or via the Emergency Access account
Note 2: If making an API call from an IP Address which is not authorized, then API will return a HTTP Status Code of 403 - Forbidden

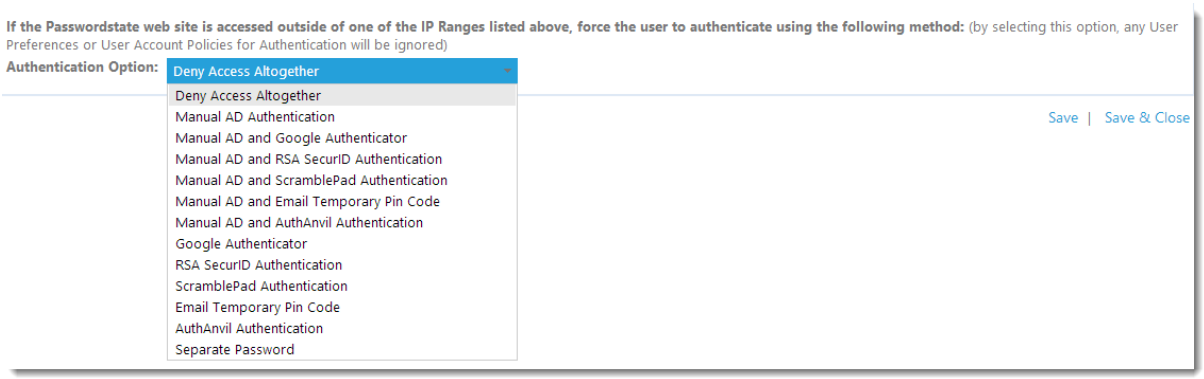
### If the Passwordstate web site is accessed outside of one of the IP Ranges listed above, force the user to authenticate using the following method

If you would like to choose a different authentication method when your users our outside of your internal network, then you can choose the option from here.

By default, access from IP Addresses which aren't listed as 'Allowed' will be blocked. By selecting an authentication option instead, you can enforce a different authentication mechanism. This is a more secure option if you use Passthrough Authentication within the office, but want to further secure access to Passwordstate when outside of the office.

Note : By selecting this option, any User Preferences or User Account Policies for Authentication will be ignored

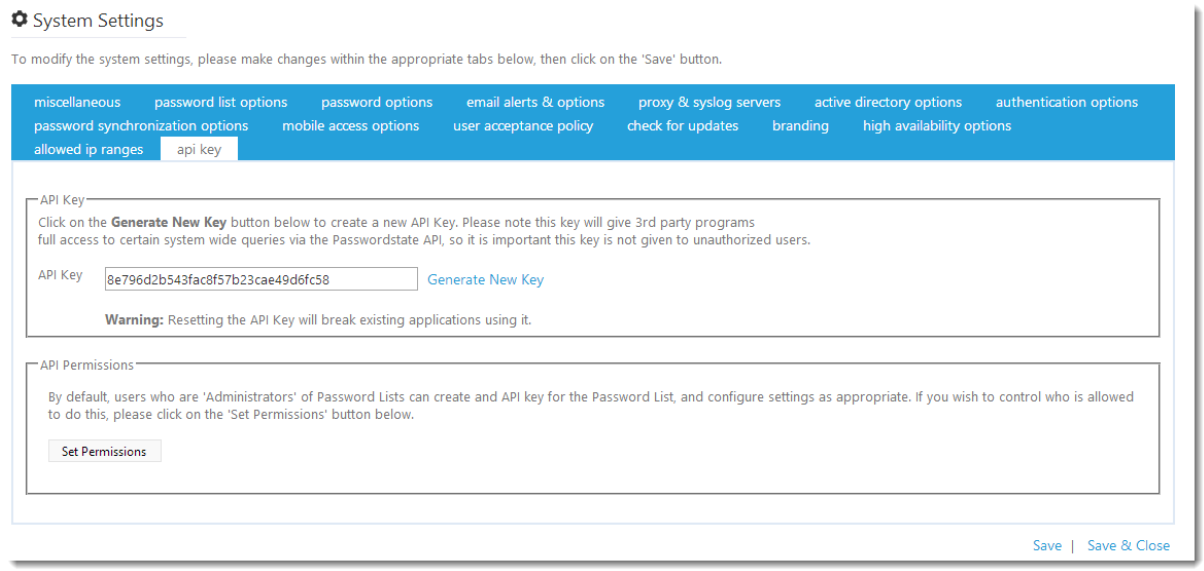
© 2014 Click Studios (SA) Pty Ltd


If the Passwordstate web site is accessed outside of one of the IP Ranges listed above, force the user to authenticate using the following method: (by selecting this option, any User Preferences or User Account Policies for Authentication will be ignored)
Authentication Option:
Deny Access Altogether
Deny Access Altogether
Manual AD Authentication
Manual AD and Google Authenticator
Manual AD and RSA SecurID Authentication
Manual AD and ScramblePad Authentication
Manual AD and Email Temporary Pin Code
Manual AD and AuthAnvil Authentication
Google Authenticator
RSA SecurID Authentication
ScramblePad Authentication
Email Temporary Pin Code
AuthAnvil Authentication
Separate Password
Save | Save & Close

## 23.15 API Key Tab

The API Key Tab allows you to specify a System Wide API Key which can be used for various API Calls. Please refer to the API Documentation for further details.

If you don't want certain users to be able to create API Keys for Password Lists, you can specify which ones are allowed to by clicking on the 'Set Permissions' button and following the on-screen instructions. Note: Only Password List Administrators have the access to create/configure API Keys for Password Lists.


System Settings
To modify the system settings, please make changes within the appropriate tabs below, then click on the 'Save' button.
miscellaneous
password list options
password options
email alerts & options
proxy & syslog servers
active directory options
authentication options
password synchronization options
mobile access options
user acceptance policy
check for updates
branding
high availability options
allowed ip ranges
api key
API Key
Click on the Generate New Key button below to create a new API Key. Please note this key will give 3rd party programs full access to certain system wide queries via the Passwordstate API, so it is important this key is not given to unauthorized users.
API Key
8e796d2b543fac8f57b23cae49d6fc58
Generate New Key
Warning: Resetting the API Key will break existing applications using it.
API Permissions
By default, users who are 'Administrators' of Password Lists can create and API key for the Password List, and configure settings as appropriate. If you wish to control who is allowed to do this, please click on the 'Set Permissions' button below.
Set Permissions
Save | Save & Close

# 24 User Accounts

Prior to any of your users being able to access the Passwordstate web site, you must first register their accounts in the User Accounts screen.

There 4 different ways user accounts can be added to Passwordstate, and they are:

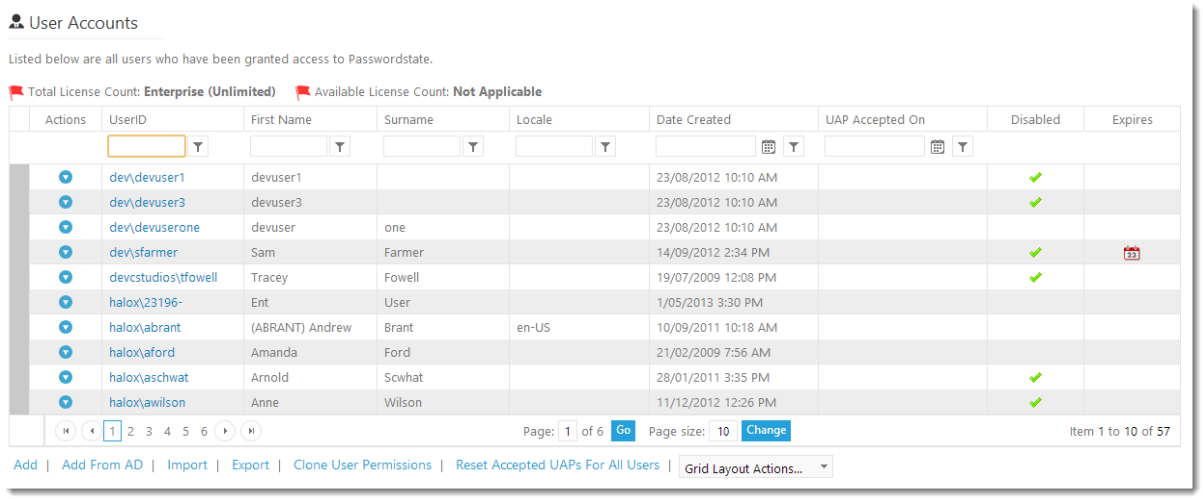
- Adding them manually by clicking on the 'Add' button

© 2014 Click Studios (SA) Pty Ltd

- Importing them from Active Directory by clicking on the 'Add from AD' button
- Importing them from a csv file by clicking on the Import button
- Or, when membership of an Active Directory Security Groups is synchronized - please see the Security Groups screen for information on this method

Performance Tip: If you have many Active Directory User Accounts added to Passwordstate, the synchronization features on the Active Directory Options Tab on the System Settings page will perform significantly better if these user accounts belong to one or more Security Groups, and these Security Groups have also been added to Passwordstate via the page Security Groups. The reason for this performance improvement is because all the users can be enumerated with one call to Active Directory for the Security Group, instead of making separate calls for every single account. If you have many AD users added to Passwordstate (i.e. 200+), it is recommended you add one or more Security Groups even if you don't use them to apply permissions anywhere.

Note: When you first add a user's account to Passwordstate, they will receive an email informing them they have access, and what URL to access the site with - assuming the email notification category is not disabled on the screen Email Templates.


User Accounts
Listed below are all users who have been granted access to Passwordstate.
Total License Count: Enterprise (Unlimited)
Available License Count: Not Applicable
Actions
UserID
First Name
Surname
Locale
Date Created
UAP Accepted On
Disabled
Expires
dev\devuser1 devuser1 23/08/2012 10:10 AM
dev\devuser3 devuser3 23/08/2012 10:10 AM
dev\devuserone devuser one 23/08/2012 10:10 AM
dev\sfarmer Sam Farmer 14/09/2012 2:34 PM
devcstudios\tfowell Tracey Fowell 19/07/2009 12:08 PM
halox\23196- Ent User 1/05/2013 3:30 PM
halox\abrant (ABRANT) Andrew Brant en-US 10/09/2011 10:18 AM
halox\aford Amanda Ford 21/02/2009 7:56 AM
halox\aschwat Arnold Scwhat 28/01/2011 3:35 PM
halox\awilson Anne Wilson 11/12/2012 12:26 PM
1 2 3 4 5 6
Page: 1 of 6 Go
Page size: 10 Change
Item 1 to 10 of 57
Add | Add From AD | Import | Export | Clone User Permissions | Reset Accepted UAPs For All Users | Grid Layout Actions...

Once you have added the user's account to Passwordstate, there are certain functions which can be performed against it.

## Local Login Accounts

When using the Active Directory Integrated version of Passwordstate, it's still possible to create Local Login Accounts, which aren't tied to Active Directory. This would only ever get used in rare circumstances when you have users wanting to use Passwordstate, but don't have an AD Account. In order to take advantage of this feature you need to:

- For the Passwordstate web site in IIS, you need to set the Authentication for the site to 'Anonymous'
- You need to add, or import via a csv file, 'Local Login Accounts' to Passwordstate - these behave

© 2014 Click Studios (SA) Pty Ltd

similar to Forms-Based accounts

Note: There are some limitations when you configure Passwordstate in this manner. In particular, user's won't be able to set their own Authentication options in the Preferences screen, Security Administrators won't be able to configure any Authentication options for a User Account Policy, and certain System Wide Authentication options will also be disabled.

## User Account Actions Menu

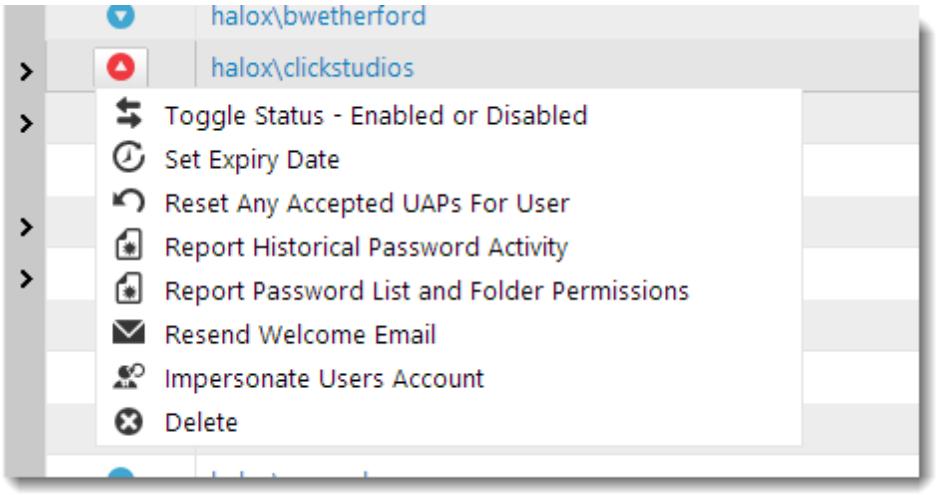
The following 'Actions' menu items are available for a user's account:

- Toggle Status (Enabled or Disabled) - this will either enable or disable the user's account, preventing them from accessing the Passwordstate web site
- Set Expiry Date - it is possible to set a date in which the user's account can either by disabled, or deleted from Passwordstate. This is a useful feature if you know an employee is leaving the organization on a specific date
- Reset any Accepted UAPs for User - If needed, it's possible to reset the 'accepted' status of the User Acceptance Policy for a user. The User Acceptance Policy can be configured on the screen System Settings -> User Acceptance Policy Tab
- Report Historical Password Activity - this reports shows all auditing data for the user's account as it relates to password records i.e. viewing passwords, copying to the clipboard, access permissions, etc
- Report Password List and Folder Permissions - this report will show all the Password Lists and Folders the user has access to, and what their permissions are. The permissions are either based on their own individual user account, or any security groups they may be members of
- Resend Welcome Email - if you need to resend the initial Welcome email to the user (the email they first receive when their account is first added to Passwordstate), then you can use this menu item
- Impersonate Users Account - this feature should only be used when trying to troubleshoot issues with the affected user. By selecting this option, an email will be send to the user informing them you are "impersonating" them, as we as to all Security Administrators. Audit records are also added. When you are impersonating a user, being able to see, edit or add passwords will be disabled
- Delete - deleting a user's account will remove all access for them, so please use with caution

Note 1 : The status (enabled or disabled) of a user's account may also change depending on the Active Directory synchronization settings on the screen System Settings -> Active Directory Options Tab

Note 2 : Disabling a user's account does not count towards the number of used licenses

© 2014 Click Studios (SA) Pty Ltd




## Editing User Account Settings

By clicking on the UserID hyperlink in the grid, you will be directed to a screen where you can edit multiple properties for the user's account.

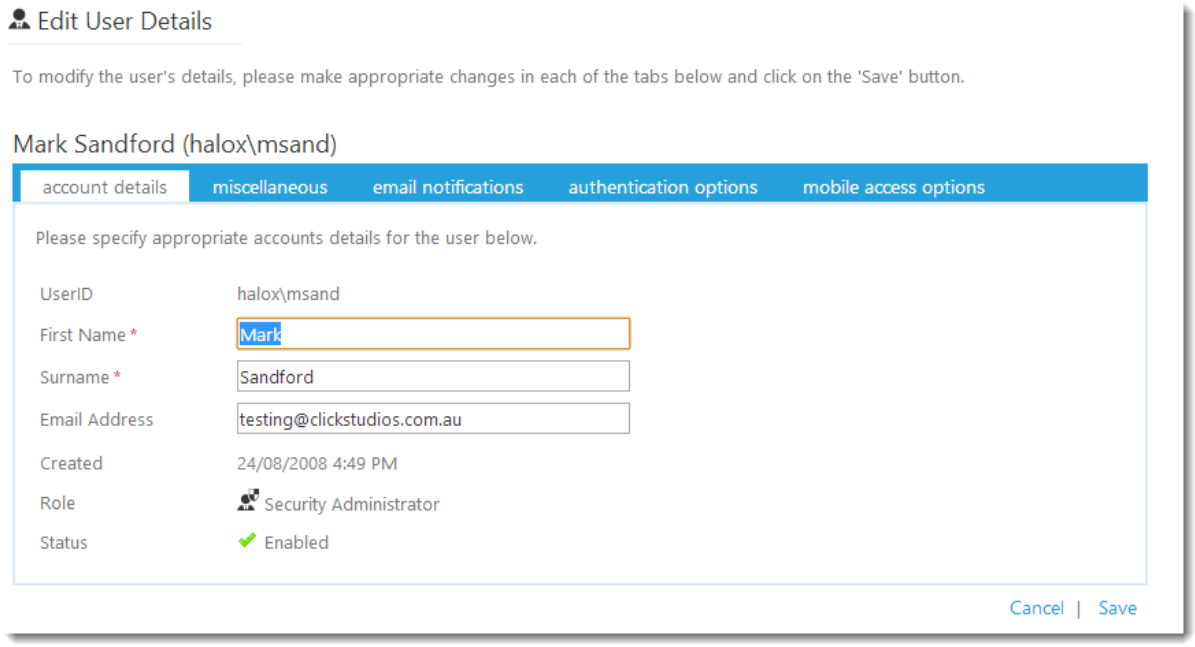
Note 1: Any changes to a user's account will not be in effect until the user logs off, then back in to the Passwordstate web site.
Note 2: The Miscellaneous, Email Notifications and Authentication Options tabs are almost identical to what the user sees when they view their own Preferences
Note 3: User Account Policies may override any number of settings for the user, in which case the relevant controls on each of the tabs will be disabled

## Account Details Tab

The Account Details Tab has some basic information about the user's account which you can edit, but should rarely need to be touched.

Note: At this stage it's not possible to rename a user's UserID value due to the way this field is encrypted throughout a lot of the tables in the Passwordstate database.

© 2014 Click Studios (SA) Pty Ltd




## Miscellaneous Tab

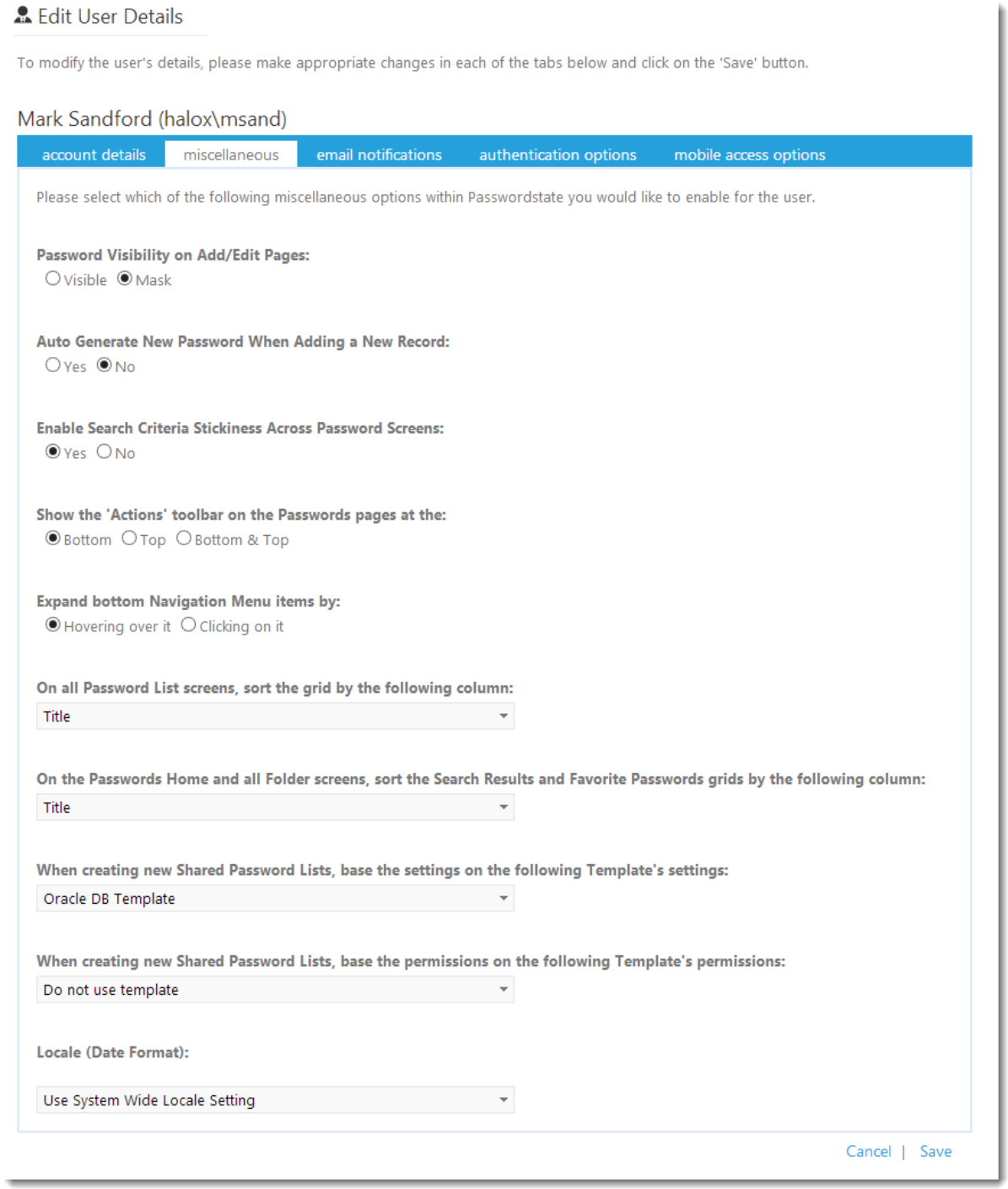
The Miscellaneous Tab has the following settings you can choose for the user:

| | |
|---|---|
| Password Visibility on Add/View/Edit Pages | When you add a new Password or edit an existing one, by default the password value is masked i.e. ****** If you choose, you can instead show the password value instead of the masked one |
| Auto Generate New Password When Adding a New Record | When adding a new Password record, you can automatically generate a new random password instead of having to specify one yourself. The format/ complexity of the new random password will be determined by which Password Generator Policy is applied to the Password List |
| Enable Search Criteria Stickiness Across Password Screens | When using the search textbox found at the top of most Password screens, you can choose to make this search value you type sticky across different Password Lists i.e. if you search for 'test' in one Password List, when you click on another Password List in the Navigation Tree, the contents of the Passwords grid will also be filtered by the term 'test'. You can also clear the search criteria by clicking on the icon |
| Show the 'Actions' toolbar on the Passwords pages at the | At the bottom of every Passwords grid there are certain buttons/controls for adding passwords, importing them, viewing documents, etc. With this option, you can choose to display the 'Actions' toolbar at the |

© 2014 Click Studios (SA) Pty Ltd

| | |
|---|---|
| | bottom of the Passwords grid, at the top, or both |
| Expand bottom Navigation Menu items by | The Navigation Menu at the bottom of the screen can expand certain menus vertically by simply hovering over them. If you choose, you can change this option so you must first click on the Menu item before it expands |
| On all Password List screens, sort the grid by the following column | If you would like all Password grids to be sorted by default on a selected column, you can choose the column here. Note: this will override you manually sorting a column and then selecting the save the Grid layout |
| On the Passwords Home and all Folder screens, sort the Search Results and Favorite Passwords grids by the following column | Similar to the option above, but this sort order applies to the Search Results and Favorite Passwords grids on the Passwords Home page and and Folder pages |
| When creating new Shared Password Lists, base the settings on the following Template's settings | When creating new Password Lists, you can choose to automatically specify all the settings based on one of the Templates you select here |
| When creating new Shared Password Lists, base the permissions on the following Template's permissions | When creating new Password Lists, you can choose to automatically base all the permissions on one of the Templates you select here |
| Locale (Date Format) | Allows you to specify a date format for any date fields - you may need different format based on your region, compared to that of what Passwordstate is current set to use system wide |

© 2014 Click Studios (SA) Pty Ltd

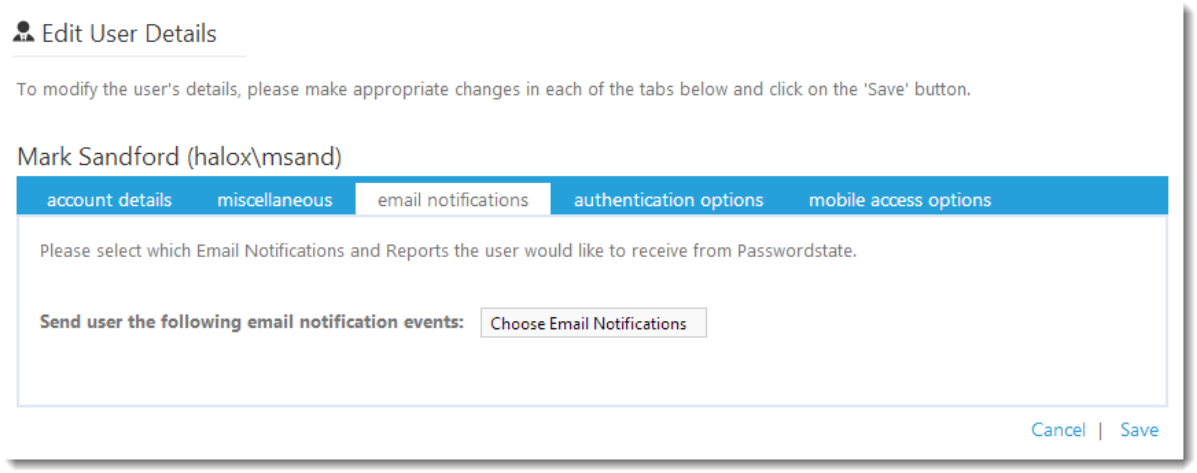

Edit User Details
To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.
Mark Sandford (halox\msand)
account details
miscellaneous
email notifications
authentication options
mobile access options
Please select which of the following miscellaneous options within Passwordstate you would like to enable for the user.
Password Visibility on Add/Edit Pages:
Visible
Mask
Auto Generate New Password When Adding a New Record:
Yes
No
Enable Search Criteria Stickiness Across Password Screens:
Yes
No
Show the 'Actions' toolbar on the Passwords pages at the:
Bottom
Top
Bottom & Top
Expand bottom Navigation Menu items by:
Hovering over it
Clicking on it
On all Password List screens, sort the grid by the following column:
Title
On the Passwords Home and all Folder screens, sort the Search Results and Favorite Passwords grids by the following column:
Title
When creating new Shared Password Lists, base the settings on the following Template's settings:
Oracle DB Template
When creating new Shared Password Lists, base the permissions on the following Template's permissions:
Do not use template
Locale (Date Format):
Use System Wide Locale Setting
Cancel | Save

## Email Notifications Tab

The Email Notifications Tab allows you to enabled/disabled one or more of the many different email notifications Passwordstate can send to the user, as well as different report options.

© 2014 Click Studios (SA) Pty Ltd

Note 1: The feature Email Notification Groups may cause the 'Choose Email Notifications' button below to be disabled
Note 2: One or more Email Templates may also be disabled, in which case the user will not receive email notifications for the disabled templates

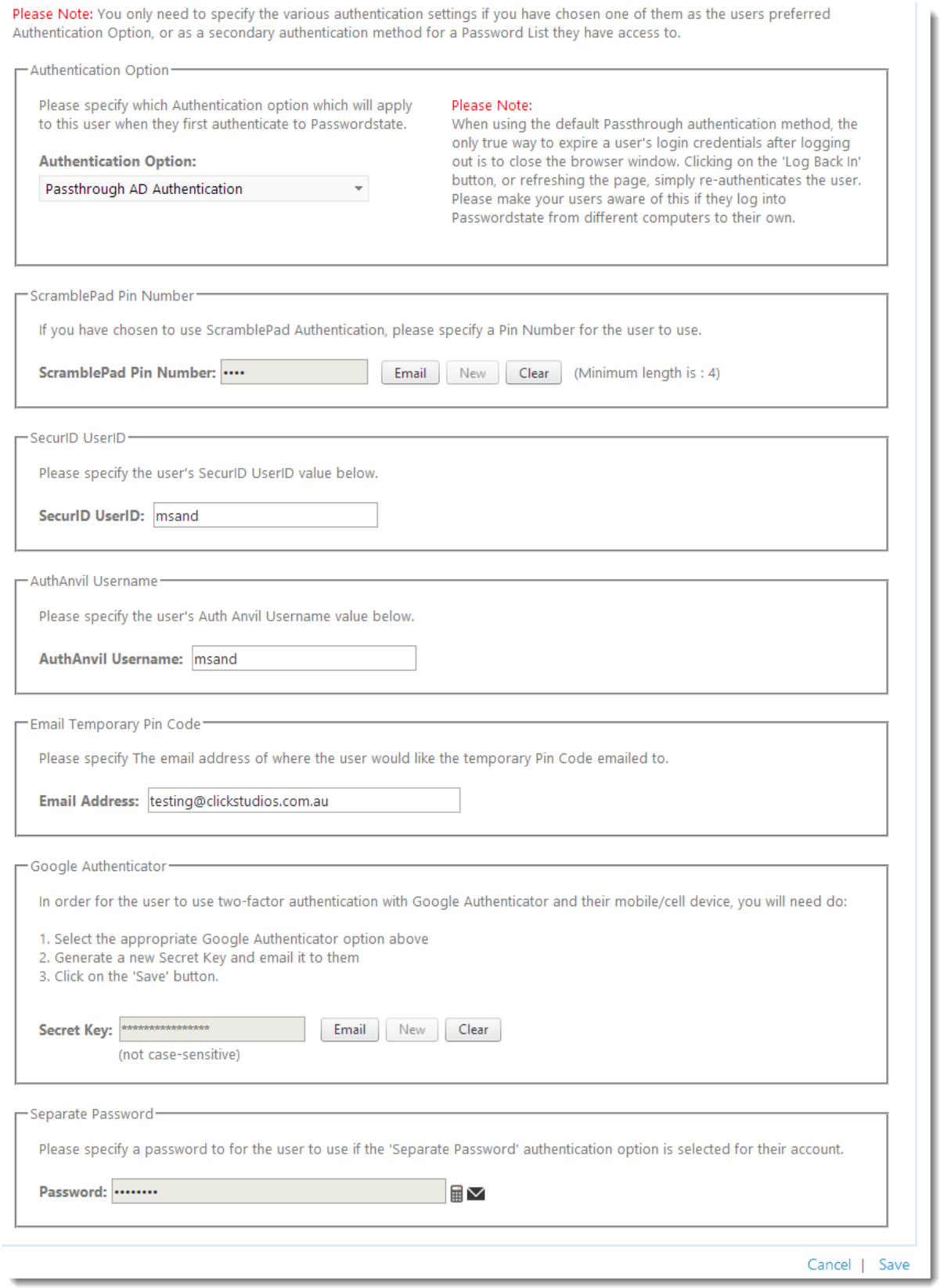

Edit User Details
To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.
Mark Sandford (halox\msand)
account details
miscellaneous
email notifications
authentication options
mobile access options
Please select which Email Notifications and Reports the user would like to receive from Passwordstate.
Send user the following email notification events:
Choose Email Notifications
Cancel | Save

## Authentication Options Tab

The Authentication Options Tab allows you to:

- Specify which Authentication Option should be used for the user's account - details and screenshots for each of the different authentication options can be found on the screen System Settings -> Authentication Options Tab
- Specify SecurID and AuthAnvil account details
- Create/clear/email the user their ScramblePad Pin number
- Create/clear/email the user their Google Authenticator Secret Key

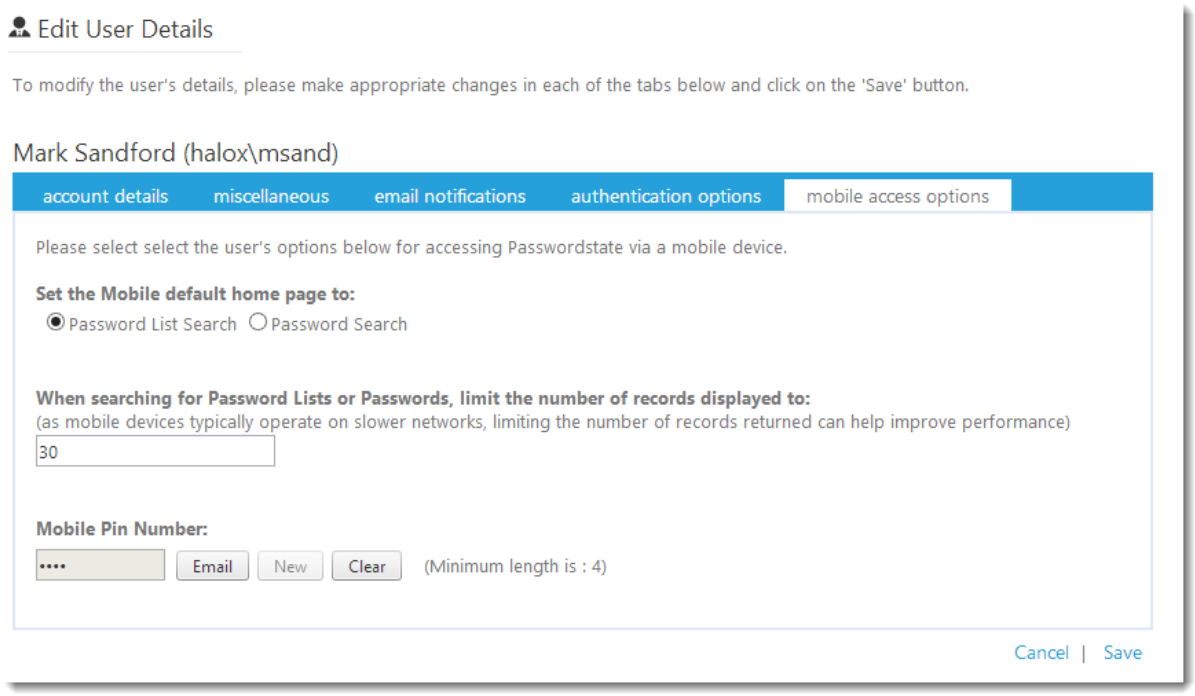
© 2014 Click Studios (SA) Pty Ltd


Please Note: You only need to specify the various authentication settings if you have chosen one of them as the users preferred Authentication Option, or as a secondary authentication method for a Password List they have access to.
Authentication Option
Please specify which Authentication option which will apply to this user when they first authenticate to Passwordstate.
Authentication Option:
Passthrough AD Authentication
Please Note:
When using the default Passthrough authentication method, the only true way to expire a user's login credentials after logging out is to close the browser window. Clicking on the 'Log Back In' button, or refreshing the page, simply re-authenticates the user. Please make your users aware of this if they log into Passwordstate from different computers to their own.
ScramblePad Pin Number
If you have chosen to use ScramblePad Authentication, please specify a Pin Number for the user to use.
ScramblePad Pin Number:
Email
New
Clear
(Minimum length is : 4)
SecurID UserID
Please specify the user's SecurID UserID value below.
SecurID UserID:
msand
AuthAnvil Username
Please specify the user's Auth Anvil Username value below.
AuthAnvil Username:
msand
Email Temporary Pin Code
Please specify The email address of where the user would like the temporary Pin Code emailed to.
Email Address:
testing@clickstudios.com.au
Google Authenticator
In order for the user to use two-factor authentication with Google Authenticator and their mobile/cell device, you will need do:
1. Select the appropriate Google Authenticator option above
2. Generate a new Secret Key and email it to them
3. Click on the 'Save' button.
Secret Key:
Email
New
Clear
(not case-sensitive)
Separate Password
Please specify a password to for the user to use if the 'Separate Password' authentication option is selected for their account.
Password:
Cancel | Save

© 2014 Click Studios (SA) Pty Ltd

## Mobile Access Options Tab

The Mobile Access Options tab allows you to specify various Mobile Client settings for the user, and to also set their Mobile Pin Number for them if required. The Pin Number can then be emailed to their account.


Edit User Details
To modify the user's details, please make appropriate changes in each of the tabs below and click on the 'Save' button.
Mark Sandford (halox\msand)
account details
miscellaneous
email notifications
authentication options
mobile access options
Please select select the user's options below for accessing Passwordstate via a mobile device.
Set the Mobile default home page to:
Password List Search
Password Search
When searching for Password Lists or Passwords, limit the number of records displayed to:
(as mobile devices typically operate on slower networks, limiting the number of records returned can help improve performance)
30
Mobile Pin Number:
Email
New
Clear
(Minimum length is : 4)
Cancel | Save

## Clone User Permissions

It's possible to clone one user's permissions to another, by using the 'Clone User Permissions' feature. This feature is generally used in one of two ways:

- You've had a new employee start who has replaced another employee, and you wish to give them the same access
- If you need to modify the UserID for a user i.e. a Domain Migration, someone gets married, etc.

Note 1: When cloning occurs, the Destination User's permissions are first removed – otherwise duplication would occur

Note 2: You need to decide of the Source user's Private Password Lists should be moved across to the Destination user. This should only ever be done if the Source and Destination user are the same actual person. The reason we provide the option to move a user's Personal Password Lists, is because a users Personal Password Lists are deleted if their account is removed from Passwordstate

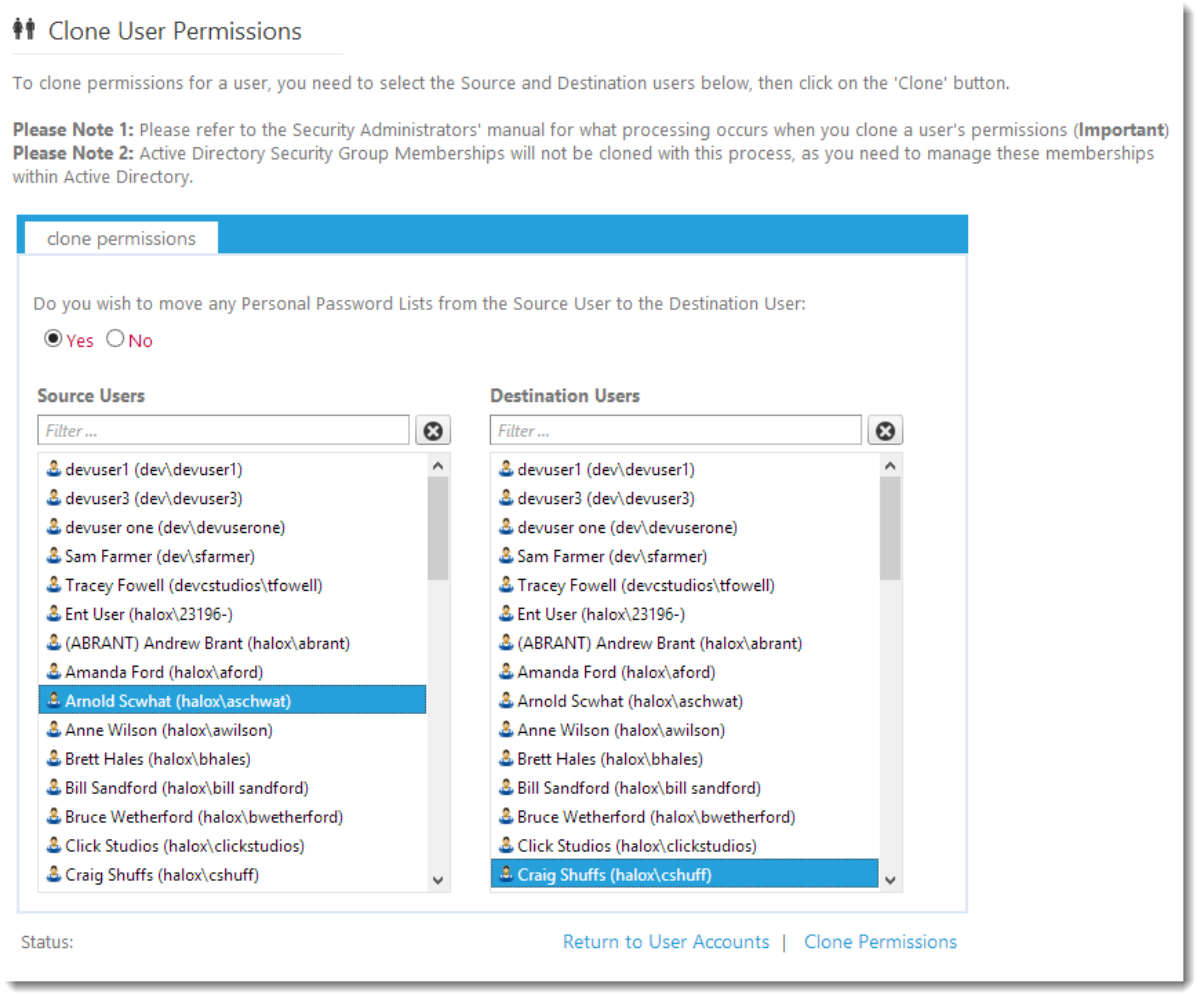
Note 3: Active Directory Security Group Memberships will not be cloned with this process, as you need to manage these memberships within Active Directory.

© 2014 Click Studios (SA) Pty Ltd

During the cloning process, the following types of permissions will be cloned:

- Any Blocked Email Notification settings
- Any memberships to Email Notification Groups
- Any Favorite Passwords
- Any of the 'Features' permissions for what menus the user is allowed access to at the bottom of the screen
- Any Grid Settings – which columns to see, width, etc.
- Any permissions to Password Lists (auditing records are added)
- Any Password Permissions (auditing records are added)
- Any permissions to Password Lists Templates (auditing records are added)
- Any Security Admin Roles (auditing records are added)
- Any membership to Local Security Groups (auditing records are added)
- The expand/collapse status of the Password Lists Navigation Tree
- Any User Account Policy permissions
- Any Scheduled Reports

© 2014 Click Studios (SA) Pty Ltd


Clone User Permissions
To clone permissions for a user, you need to select the Source and Destination users below, then click on the 'Clone' button.
Please Note 1: Please refer to the Security Administrators' manual for what processing occurs when you clone a user's permissions (Important)
Please Note 2: Active Directory Security Group Memberships will not be cloned with this process, as you need to manage these memberships within Active Directory.
clone permissions
Do you wish to move any Personal Password Lists from the Source User to the Destination User:
Yes No
Source Users
Filter ...
devuser1 (dev\devuser1)
devuser3 (dev\devuser3)
devuser one (dev\devuserone)
Sam Farmer (dev\sfarmer)
Tracey Fowell (devcstudios\tfowell)
Ent User (halox\23196-)
(ABRANT) Andrew Brant (halox\abrant)
Amanda Ford (halox\aford)
Arnold Scwhat (halox\aschwat)
Anne Wilson (halox\awilson)
Brett Hales (halox\bhales)
Bill Sandford (halox\bill sandford)
Bruce Wetherford (halox\bwetherford)
Click Studios (halox\clickstudios)
Craig Shuffs (halox\cshuff)
Destination Users
Filter ...
devuser1 (dev\devuser1)
devuser3 (dev\devuser3)
devuser one (dev\devuserone)
Sam Farmer (dev\sfarmer)
Tracey Fowell (devcstudios\tfowell)
Ent User (halox\23196-)
(ABRANT) Andrew Brant (halox\abrant)
Amanda Ford (halox\aford)
Arnold Scwhat (halox\aschwat)
Anne Wilson (halox\awilson)
Brett Hales (halox\bhales)
Bill Sandford (halox\bill sandford)
Bruce Wetherford (halox\bwetherford)
Click Studios (halox\clickstudios)
Craig Shuffs (halox\cshuff)
Status:
Return to User Accounts | Clone Permissions

## Reset Accepted UAPs for All Users

It's also possible to reset the status of accepted User Acceptance Policies for your users as well. It's possible you will want to do this periodically, as you may need to modify the policy based on business requirements. Resetting this accepted value means the user will be prompted again to read and accept the updated policy - assuming you have this option enabled on the System Settings User Acceptance Policy Tab. In the User Accounts grid as well, you can see the data and time each of the users last accepted the User Acceptance Policy.

# 25 User Account Policies

User Account Policies allow you to manage a specific set of settings for a groups of users at a time. The settings relate to various User Preferences, and how the Password Lists, Password Folders and Home Page screens appear to the user.

© 2014 Click Studios (SA) Pty Ltd

An example of how User Account Policies can be used is to hide all graphs on all screens from the users.

When a User Account Policy is applied to a user's account, the controls/settings on the screen will be disabled, informing the user a User Account Policy is in effect for their account.

## Adding a User Account Policy

When you add a User Account Policy, you can choose to set any number of the following settings:

**User Preferences**

| |
|---|
| Mask Password Visibility on Add/View/Edit Pages |
| Auto Generate New Password When Adding a New Record |
| Enable Search Criteria Stickiness Across Password Screens |
| Show the 'Actions' toolbar on the Passwords pages at the |
| Expand the bottom Navigation Menu items by |
| Locale (Date Format) |
| Specify which Authentication option will apply to the user's account |

**Password List Screen Options**

| |
|---|
| Show the 'Header' row on all Passwords Grids |
| Show the 'Filter' controls in the Header of the Passwords Grids |
| Show the 'Header' row on all Recent Activity Grids |
| Make the Recent Activity Grid visible to the user |
| Selects the Paging Style controls for Password and Recent Activity grids |
| Make the Pie Charts visible to the user |
| Sort the grid by the following column |

**Home Page and Folder Screen Options**

| |
|---|
| Show the Favorites Passwords Grid |
| Show the Password Statistics Chart |
| Choose the Style of the Password Statistics Chart |
| Stack the data points on top of each other for the Password Statistics Chart |
| Select the color theme for the Password Statistics Chart |
| Sort the Search Results and Favorite Passwords grids by the following column |

**Mobile Access Options**

| |
|---|
| Set the Mobile default home page to |
| When searching for Password Lists or Passwords, limit the number of records displayed to |

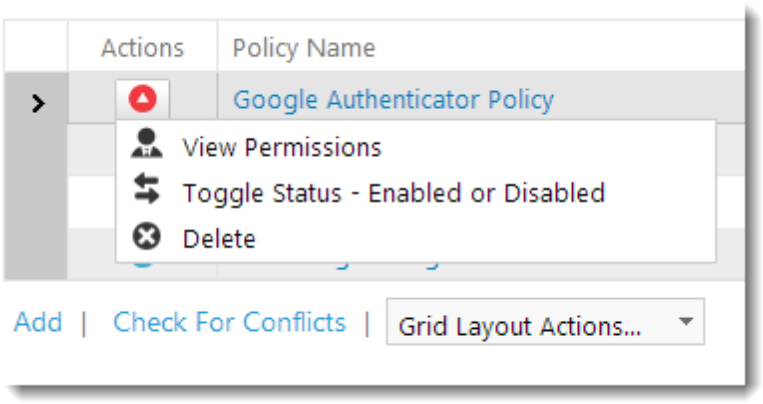
Note: When you first add a new User Account Policy, it is disabled by default. It is recommended that before you enable the policy, you apply the permissions required, then click on the 'Check for Conflicts' button. The Check for Conflicts process will ensure that there are no two settings with different values assigned to a user's account - this could cause confusion for the user, and for Security Administrators if this is the case.

© 2014 Click Studios (SA) Pty Ltd

## User Account Policy Actions

Once you have created a Policy with the desired settings, the following Actions Menu items are available to you:

- View Permissions - allows you to view, and make permission changes as to who the policy is in effect for
- Toggle Status - either enable or disable the policy
- Delete - delete the policy




© 2014 Click Studios (SA) Pty Ltd